

**IN THE UNITED STATES DISTRICT COURT  
FOR THE EASTERN DISTRICT OF TEXAS  
MARSHALL DIVISION**

**TQP DEVELOPMENT, LLC**

Plaintiff,

v.

- (1) **MERRILL LYNCH & CO., INC.**
- (2) **BANK OF AMERICA CORP.;**
- (3) **BANK OF AMERICA, N.A.;**
- (4) **CAPITAL ONE FINANCIAL CORPORATION;**
- (5) **CAPITAL ONE SERVICES, INC.;**
- (6) **CAPITAL ONE, NA;**
- (7) **COMERICA INCORPORATED;**
- (8) **COMERICA BANK AND TRUST, NA;**
- (9) **CITIGROUP INC.;**
- (10) **PRIMERICA FINANCIAL SERVICES, INC.;**
- (11) **CITIBANK NA;**
- (12) **CITIGROUP GLOBAL MARKETS INC. D/B/A SMITH BARNEY**
- (13) **E\*TRADE FINANCIAL CORPORATION;**
- (14) **FIDELITY INVESTMENTS, INC.**
- (15) **FMR LLC;**
- (16) **FMR CORP.;**
- (17) **THE GOLDMAN SACHS GROUP, INC.;**
- (18) **GOLDMAN, SACHS & CO.;**
- (19) **ING GROEP N.V.;**
- (20) **ING BANK FSB;**
- (21) **SHAREBUILDER SECURITIES CORPORATION**
- (22) **SHAREBUILDER CORPORATION;**
- (23) **MORGAN STANLEY;**
- (24) **MORGAN STANLEY & CO., INC.;**
- (25) **THE ROYAL BANK OF SCOTLAND GROUP PLC;**
- (26) **CITIZENS FINANCIAL GROUP, INC.;**
- (27) **RBS CITIZENS, N.A.;**
- (28) **JPMORGAN CHASE & CO.;**

**Civil Action No. \_\_\_\_\_**

**JURY TRIAL DEMANDED**

- (29) **JPMORGAN CHASE BANK NA;**
  - (30) **RAYMOND JAMES FINANCIAL,**  
**INC.;**
  - (31) **TD AMERITRADE HOLDING**  
**CORPORATION;**
  - (32) **TD AMERITRADE, INC.;**
  - (33) **REGIONS FINANCIAL**  
**CORPORATION;**
  - (34) **NATIONAL CITY CORPORATION;**
  - (35) **NATIONAL CITY BANK;**
  - (36) **INTERNATIONAL BANCSHARES**  
**CORPORATION;**
  - (37) **IBC SUBSIDIARY CORPORATION;**
  - (38) **INTERNATIONAL BANK OF**  
**COMMERCE;**
  - (39) **AMEGY CORPORATION;**
  - (40) **AMEGY BANK, NA D/B/A AMEGY**  
**BANK OF TEXAS;**
  - (41) **FIFTH THIRD BANCORP; AND**
  - (42) **FIFTH THIRD BANK.**
- Defendants.

### **COMPLAINT FOR PATENT INFRINGEMENT**

This is an action for patent infringement in which TQP Development, LLC (“TQP”). makes the following allegations against Merrill Lynch & Co., Inc., Bank of America Corp., Bank of America, N.A., Capital One Financial Corporation, Capital One Services, Inc., Capital One, National Association, Comerica Incorporated, Comerica Bank and Trust, NA, Citigroup Inc., Primerica Financial Services, Inc., Citibank, NA, Citigroup Global Markets Inc. d/b/a Smith Barney, E\*Trade Financial Corporation, Fidelity Investments, Inc., FMR LLC, FMR Corp., The Goldman Sachs Group, Inc., Goldman, Sachs & Co., ING Groep N.V., ING Bank FSB, ShareBuilder Securities Corporation, ShareBuilder Corporation, Morgan Stanley, Morgan Stanley & Co. Inc., The Royal Bank of Scotland Group PLC, Citizens Financial Group, Inc., RBS Citizens, N.A., JPMorgan Chase & Co., JPMorgan Chase Bank NA, Raymond James Financial, Inc., TD AMERITADE Holding Corporation, TD AMERITRADE, Inc., Regions

Financial Corporation, National City Corporation, National City Bank, International Bancshares Corporation, IBC Subsidiary Corporation, International Bank of Commerce, Amegy Corporation, Amegy Bank, NA d/b/a Amegy Bank of Texas, Fifth Third Bancorp, and Fifth Third Bank (collectively the “Defendants”).

### **PARTIES**

1. Plaintiff TQP Development, LLC. is a Texas limited liability company having a principal place of business of 207C North Washington Street, Marshall, Texas 75670.

2. On information and belief, Defendant Merrill Lynch & Co., Inc. (“Merrill Lynch”) is a Delaware corporation with its principal place of business at 4 World Financial Center, New York, New York 10080. Merrill Lynch has appointed The Corporation Trust Company, Corporation Trust Center, 1209 Orange Street, Wilmington, DE 19801, as its agent for service of process.

3. On information and belief, Defendant Bank of America Corporation. (“BOA”) is a Delaware corporation with its principal place of business at 100 N. Tryon Street, Charlotte, NC 28255. BOA is qualified to do business in the State of Texas and has appointed CT Corporation System, 350 N. St. Paul Street, Dallas, TX 75201, as its agent for service of process.

4. On information and belief, Defendant Bank of America, NA. (“BOA NA”) is a subsidiary of BOA with its principal place of business at 100 Tryon Street, Charlotte, NC 28255. BOA NA may be served through its registered agent at CT Corporation System, 350 N. St. Paul Street, Dallas, TX 75201.

5. On information and belief, Defendant Capital One Financial Corporation, (“Capital”) is a Delaware corporation with its principal place of business at 1680 Capital One Drive, McLean, Virginia 22102. Capital is qualified to do business in the State of Texas and has appointed Corporation Service Company, 701 Brazos Street, Suite 1050, Austin, TX 78701, as its agent for service of process.

6. On information and belief, Defendant Capital One Services, Inc (“Capital One”) is a subsidiary of Capital with its principal place of business at 1680 Capital One Drive, McLean, Virginia 22102. Capital One may be served at Corporation Service Company, 701 Brazos Street, Suite 1050, Austin, Texas 78701.

7. On information and belief, Defendant Capital One National Association (“Capital One NA”) is a subsidiary of Capital with its principal place of business at 1680 Capital One Drive, McLean, Virginia 22102. Capital One NA may be served at Corporation Service Company, 701 Brazos Street, Suite 1050, Austin, Texas 78701.

8. On information and belief, Defendant Comerica Incorporated (“Comerica”) is a Delaware corporation, with its principal place of business at 1717 Main Street, MC 6404, Dallas, TX 75201. Comerica has appointed CT Corporation System, 350 North St. Paul Street, Dallas, TX 75201 as its registered agent.

9. On information and belief, Defendant Comerica Bank and Trust, National Association (“Comerica Bank”) is a subsidiary of Comerica Incorporated, with its principal place of business at 1717 Main Street, MC 6404, Dallas, TX 75201. Comerica Bank may be served at CT Corporation System, 350 North St. Paul Street, Dallas, TX 75201.

10. On information and belief, Defendant Citigroup Inc. (“Citigroup”) is a Delaware corporation with its principal place of business at 399 Park Avenue, New York, NY 10043.

Citigroup has appointed The Corporation Trust Company, Corporation Trust Center, 1209 Orange Street, Wilmington, DE 19801 as its registered agent.

11. On information and belief, Defendant Primerica Financial Services, Inc. (“Primerica”) is a subsidiary of Citigroup, Inc., with its principal place of business at 3120 Breckinridge Boulevard, Duluth, Georgia 30099. Primerica has appointed Maureen Middleton, 3100 Breckinridge Boulevard, Duluth, Georgia 30099 as its registered agent.

12. On information and belief, Defendant Citibank, NA (“Citibank”) is a commercial bank and wholly owned subsidiary of Citigroup Inc., with its principal place of business at 399 Park Avenue, New York, NY 10043. Citibank may be served through its registered agent at The Corporation Trust Company, Corporation Trust Center, 1209 Orange Street, Wilmington, DE 19801.

13. On information and belief, Defendant Citigroup Global Markets, Inc. d/b/a Smith Barney (“Smith Barney”) is a wholly owned subsidiary of Citigroup, Inc. with its principal place of business at 388 Greenwich Street, New York, New York 10013. Smith Barney can be served at Citigroup Global Market, Inc., Attn: General Counsel, 388 Greenwich Street, New York, New York 10013.

14. On information and belief, Defendant E\*Trade Financial Corporation (“E\*Trade”) is a Delaware corporation with its principal place of business at 135 East 57th Street, New York, New York 10022. E\*Trade has appointed Corporation Service Company, 2711 Centerville Road, Suite 400, Wilmington, DE 19808 as its registered agent.

15. On information and belief, Defendant Fidelity Investments, Inc. (“Fidelity”) is a Texas corporation with its principal place of business at 10120 Desert Willow Drive, Dallas, TX

75243. Fidelity has appointed Daniel C Lemay, 2921 Suffolk Court East, Suite 350, Fort Worth, TX 76133 as its registered agent.

16. On information and belief, Defendant FMR LLC (“FMR LLC”) is a Delaware limited liability company with its principal place of business at 82 Devonshire Street, Boston, MA 02109. FMR LLC has appointed The Corporation Trust Company, Corporation Trust Center, 1209 Orange Street, Wilmington, DE 19801 as its registered agent.

17. On information and belief, Defendant FMR Corp. (“FMR Corp.”) is a Delaware corporation with its principal place of business at 82 Devonshire Street, Boston, MA 02109. FMR Corp. has appointed The Corporation Trust Company, Corporation Trust Center, 1209 Orange Street, Wilmington, DE 19801 as its registered agent.

18. On information and belief, Defendant The Goldman Sachs Group, Inc. (“Goldman Sachs”) is a Delaware corporation with its principal place of business at 85 Broad Street, New York, NY 10004. Goldman Sachs has appointed The Corporation Trust Company, Corporation Trust Center, 1209 Orange Street, Wilmington, DE 19801, as its agent for service of process.

19. On information and belief, Defendant Goldman, Sachs & Co. (“GS & Co.”) is a New York corporation with its principal place of business at 85 Broad Street, New York, NY 10004. GS & Co. may be served at 85 Broad Street, New York, NY 10004.

20. On information and belief, Defendant ING Groep N.V. (“ING”) is a Netherlands company with its principal place of business at Amstelveenseweg 500, 1081 KL Amsterdam, P.O. Box 810, 1000 AV Amsterdam, The Netherlands.

21. On information and belief, Defendant ING Bank fsb, d/b/a ING Direct Bancorp, a subsidiary of ING Groep N.V., (“ING Bank”) is a federally chartered savings bank with its

principal place of business at 1 S. Orange Street, Wilmington, DE 19801. ING Bank has appointed Deneed Donnley-Evans, 1 S. Orange Street, Wilmington, DE 19801, as its agent for service of process.

22. On information and belief, Defendant ShareBuilder Securities Corporation, a subsidiary of ING Bank fsb d/b/a ING Direct Bancorp, (“ShareBuilder Securities”) is a Washington corporation with its principal place of business at 1445 120<sup>th</sup> Avenue NE, Bellevue, WA 98005. ShareBuilder Securities has appointed Corporation Service Company, 6500 Harbour Heights Pwky., Suite 400, Mukilteo, WA 98275, as its agent for service of process.

23. On information and belief, Defendant ShareBuilder Corporation, a subsidiary of ING Bank fsb d/b/a ING Direct Bancorp, (“ShareBuilder”) is a Washington corporation with its principal place of business at 1445 120th Avenue NE, Bellevue, WA 98005. ShareBuilder has appointed Corporation Service Company, 6500 Harbour Heights Pwky., Suite 400, Mukilteo, WA 98275, as its agent for service of process.

24. On information and belief, Defendant Morgan Stanley (“Morgan Stanley”) is a Delaware corporation with its principal place of business at 1585 Broadway, New York, NY 10036. Citigroup has appointed The Corporation Trust Company, Corporation Trust Center, 1209 Orange Street, Wilmington, DE 19801 as its registered agent.

25. On information and belief, Defendant Morgan Stanley & Co. Inc., a subsidiary of Defendant Morgan Stanley, (“Morgan Stanley Inc.”) is a Delaware corporation with its principal place of business at 1585 Broadway, New York, NY 10036. Morgan Stanley Inc. has appointed The Corporation Trust Company, Corporation Trust Center, 1209 Orange Street, Wilmington, DE 19801 as its registered agent.

26. On information and belief, Defendant The Royal Bank of Scotland Group PLC (“RBS”) is a UK company with its principal place of business at RBS Gogarburn, PO Box 1000, Edinburgh EH12 1HQ, United Kingdom. Defendant RBS may be served via Miller McLean, Group General Counsel and Group Secretary, PO Box 1000, Gogarburn, Edinburgh EH12 1HQ.

27. On information and belief, Defendant Citizens Financial Group, Inc., a subsidiary of Defendant RBS, (“Citizens Financial”) is a Delaware corporation with its principal place of business at One Citizens Plaza, Providence, RI 02903. Citizens Financial is qualified to do business in the State of Texas and has appointed Corporation Service Company, 2711 Centerville Road, Suite 400, Wilmington, DE 19808 as its registered agent.

28. On information and belief, Defendant RBS Citizens, N.A. (“RBS Citizens”) is a subsidiary of Defendant Citizens Financial, with its principal place of business at One Citizens Plaza, Providence, RI 02903. RBS Citizens may be served via the registered agent of its parent at Corporation Service Company, 2711 Centerville Road, Suite 400, Wilmington, DE 19808 as its registered agent.

29. On information and belief, Defendant JPMorgan Chase & Co. (“Chase”) is a Delaware corporation with its principal place of business at 270 Park Avenue, New York, NY 10017. Chase is qualified to do business in the State of Texas and has appointed CT Corporation System, 350 North St. Paul Street, Dallas 75201 as its registered agent.

30. On information and belief, Defendant JPMorgan Chase Bank NA (“Chase Bank”) is a subsidiary of JP Morgan Chase & Co. with its principal place of business at 270 Park Avenue, New York, NY 10017. Chase Bank may be served through its registered agent at CT Corporation System, 350 North St. Paul Street, Dallas 75201.

31. On information and belief, Defendant Raymond James Financial, Inc. (“Raymond James”) is a Florida corporation with its principal place of business at 880 Carillon Parkway, St. Petersburg, Florida 33716. Raymond James has appointed CT Corporation System, 1200 South Pine Island Road, Plantation, FL 33324 as its registered agent.

32. On information and belief, Defendant TD AMERITRADE Holding Corporation (“TD AMERITRADE Holding”) is a Delaware corporation with its principal place of business at 4211 South 102nd Street, Omaha, Nebraska 68127. TD AMERITRADE Holding is qualified to do business in the State of Texas and has appointed Corporation Service Company, 2711 Centerville Road, Suite 400, Wilmington, DE 19808 as its registered agent.

33. On information and belief, Defendant TD AMERITRADE, Inc. d/b/a TD AMERITRADE, a subsidiary of TD AMERITRADE Holding Corporation, (“TD AMERITRADE”) is a New York corporation with its principal place of business at 4211 South 102nd Street, Omaha, Nebraska 68127. TD AMERITRADE has appointed Corporation Service Company, 80 State Street, Albany, NY 12207 as its registered agent.

34. On information and belief, Defendant Regions Financial Corporation, (“Regions”) is a Delaware corporation with its principal place of business at 1900 Fifth Avenue, Birmingham, Alabama 35203. Region is qualified to do business in the State of Texas and has appointed Corporation Service Company, 701 Brazos Street, Suite 1050, Austin, TX 78701, as its agent for service of process.

35. On information and belief, Defendant National City Corporation, (“National City”) is a Delaware corporation with its principal place of business at 1900 East Ninth Street, Room 647, Cleveland, Ohio 44114. National City has appointed C. T. Corporation System, 36 East Seventh Street, Suite 2400, Cincinnati, Ohio 45202 as its agent for service of process.

36. On information and belief, Defendant National City Bank, (“National City Bank”) is a wholly owned banking subsidiary of Defendant National City. National City Bank is qualified to do business in the State of Texas and has appointed C. T. Corporation System, 350 N. St. Paul Street, Dallas, Texas 75201 as its agent for service of process.

37. On information and belief, Defendant International Bancshares Corporation (“IBC”) is a Texas corporation with its principal place of business at 1200 San Bernardo Avenue, Laredo, Texas 78042. IBC has appointed Dennis E. Nixon, 1200 San Bernardo Avenue, Laredo, Texas 78041 as its registered agent.

38. On information and belief, Defendant IBC Subsidiary Corporation (“IBC Subsidiary”) is a Delaware corporation with its principal business location at 1200 San Bernardo Avenue, Laredo, Texas 78042. IBC Subsidiary has appointed The Corporation Trust Company, Corporation Trust Center, 1209 Orange Street, Wilmington, DE 19801 as its registered agent.

39. On information and belief, Defendant International Bank of Commerce (“IBC Bank”) is a Texas bank with its principal business location at 1200 San Bernardo Avenue, Laredo, Texas 78042. IBC Bank has appointed Corporation Trust Company, 1209 Orange St., Wilmington, Delaware 19801 as its registered agent.

40. On information and belief, Defendant Amegy Corporation (“Amegy”) is a Texas corporation with its principal business location at 440 Post Oak Parkway, Houston, Texas 77027. Amegy has appointed Corporation Service Company d/b/a CSC-Lawyers Inco., 701 Brazos Street Suite 1050, Austin, Texas 78701 as its registered agent.

41. On information and belief, Defendant Amegy Bank National Association, d/b/a Amegy Bank of Texas (“Amegy Bank”) is a Texas bank with its principal business location at

440 Post Oak Parkway, Houston, Texas 77027. Amegy Bank has appointed Lynn Lovat, 400 Post Oak Parkway, Houston, Texas 77027 as its registered agent.

42. On information and belief, Defendant Fifth Third Bancorp (“Fifth Third”) is an Ohio corporation with its principal place of business at 38 Fountain Square Plaza, Cincinnati, Ohio 45263-0001. Fifth Third has appointed Paul L. Reynolds, 38 Fountain Square Plaza, Cincinnati, Ohio 45263-0001 as its registered agent.

43. On information and belief, Defendant Fifth Third Bank (“Fifth Third Bank”) is an Ohio corporation with its principal place of business at 38 Fountain Square Plaza, Cincinnati, Ohio 45263-0001. Fifth Third Bank is qualified to do business in the State of Texas and has appointed Corporation Service Company, 701 Brazos Street, Suite 1050, Austin, Texas 78701-3232 as its registered agent.

#### **JURISDICTION AND VENUE**

44. This action arises under the patent laws of the United States, Title 35 of the United States Code. This Court has subject matter jurisdiction pursuant to 28 U.S.C. §§ 1331 and 1338(a).

45. Venue is proper in this district under 28 U.S.C. §§ 1391(c) and 1400(b). On information and belief, each Defendant has transacted business in this district, and has committed and/or induced acts of patent infringement in this district.

46. On information and belief, Defendant Merrill Lynch is subject to this Court’s specific and/or general personal jurisdiction pursuant to due process and/or the Texas Long Arm Statute, due at least to its substantial business in this forum, including: (i) at least a portion of the infringements alleged herein; and/or (ii) regularly doing or soliciting business, engaging in other

persistent courses of conduct, and/or deriving substantial revenue from goods and services provided to individuals in Texas and in this Judicial District.

47. On information and belief, Defendant BOA is subject to this Court's specific and/or general personal jurisdiction pursuant to due process and/or the Texas Long Arm Statute, due at least to its substantial business in this forum, including: (i) at least a portion of the infringements alleged herein; and/or (ii) regularly doing or soliciting business, engaging in other persistent courses of conduct, and/or deriving substantial revenue from goods and services provided to individuals in Texas and in this Judicial District.

48. On information and belief, Defendant BOA NA is subject to this Court's specific and/or general personal jurisdiction pursuant to due process and/or the Texas Long Arm Statute, due at least to its substantial business in this forum, including: (i) at least a portion of the infringements alleged herein; and/or (ii) regularly doing or soliciting business, engaging in other persistent courses of conduct, and/or deriving substantial revenue from goods and services provided to individuals in Texas and in this Judicial District.

49. On information and belief, Defendant Capital is subject to this Court's specific and/or general personal jurisdiction pursuant to due process and/or the Texas Long Arm Statute, due at least to its substantial business in this forum, including: (i) at least a portion of the infringements alleged herein; and/or (ii) regularly doing or soliciting business, engaging in other persistent courses of conduct, and/or deriving substantial revenue from goods and services provided to individuals in Texas and in this Judicial District.

50. On information and belief, Defendant Capital One is subject to this Court's specific and/or general personal jurisdiction pursuant to due process and/or the Texas Long Arm Statute, due at least to its substantial business in this forum, including: (i) at least a portion of the

infringements alleged herein; and/or (ii) regularly doing or soliciting business, engaging in other persistent courses of conduct, and/or deriving substantial revenue from goods and services provided to individuals in Texas and in this Judicial District.

51. On information and belief, Defendant Capital One NA is subject to this Court's specific and/or general personal jurisdiction pursuant to due process and/or the Texas Long Arm Statute, due at least to its substantial business in this forum, including: (i) at least a portion of the infringements alleged herein; and/or (ii) regularly doing or soliciting business, engaging in other persistent courses of conduct, and/or deriving substantial revenue from goods and services provided to individuals in Texas and in this Judicial District.

52. On information and belief, Defendant Comerica is subject to this Court's specific and/or general personal jurisdiction pursuant to due process and/or the Texas Long Arm Statute, due at least to its substantial business in this forum, including: (i) at least a portion of the infringements alleged herein; and/or (ii) regularly doing or soliciting business, engaging in other persistent courses of conduct, and/or deriving substantial revenue from goods and services provided to individuals in Texas and in this Judicial District.

53. On information and belief, Defendant Comerica Bank is subject to this Court's specific and/or general personal jurisdiction pursuant to due process and/or the Texas Long Arm Statute, due at least to its substantial business in this forum, including: (i) at least a portion of the infringements alleged herein; and/or (ii) regularly doing or soliciting business, engaging in other persistent courses of conduct, and/or deriving substantial revenue from goods and services provided to individuals in Texas and in this Judicial District.

54. On information and belief, Defendant Citigroup is subject to this Court's specific and/or general personal jurisdiction pursuant to due process and/or the Texas Long Arm Statute,

due at least to its substantial business in this forum, including: (i) at least a portion of the infringements alleged herein; and/or (ii) regularly doing or soliciting business, engaging in other persistent courses of conduct, and/or deriving substantial revenue from goods and services provided to individuals in Texas and in this Judicial District.

55. On information and belief, Defendant Primerica is subject to this Court's specific and/or general personal jurisdiction pursuant to due process and/or the Texas Long Arm Statute, due at least to its substantial business in this forum, including: (i) at least a portion of the infringements alleged herein; and/or (ii) regularly doing or soliciting business, engaging in other persistent courses of conduct, and/or deriving substantial revenue from goods and services provided to individuals in Texas and in this Judicial District.

56. On information and belief, Defendant Citibank is subject to this Court's specific and/or general personal jurisdiction pursuant to due process and/or the Texas Long Arm Statute, due at least to its substantial business in this forum, including: (i) at least a portion of the infringements alleged herein; and/or (ii) regularly doing or soliciting business, engaging in other persistent courses of conduct, and/or deriving substantial revenue from goods and services provided to individuals in Texas and in this Judicial District.

57. On information and belief, Defendant Smith Barney is subject to this Court's specific and/or general personal jurisdiction pursuant to due process and/or the Texas Long Arm Statute, due at least to its substantial business in this forum, including: (i) at least a portion of the infringements alleged herein; and/or (ii) regularly doing or soliciting business, engaging in other persistent courses of conduct, and/or deriving substantial revenue from goods and services provided to individuals in Texas and in this Judicial District.

58. On information and belief, Defendant E\*Trade is subject to this Court's specific and/or general personal jurisdiction pursuant to due process and/or the Texas Long Arm Statute, due at least to its substantial business in this forum, including: (i) at least a portion of the infringements alleged herein; and/or (ii) regularly doing or soliciting business, engaging in other persistent courses of conduct, and/or deriving substantial revenue from goods and services provided to individuals in Texas and in this Judicial District.

59. On information and belief, Defendant Fidelity is subject to this Court's specific and/or general personal jurisdiction pursuant to due process and/or the Texas Long Arm Statute, due at least to its substantial business in this forum, including: (i) at least a portion of the infringements alleged herein; and/or (ii) regularly doing or soliciting business, engaging in other persistent courses of conduct, and/or deriving substantial revenue from goods and services provided to individuals in Texas and in this Judicial District.

60. On information and belief, Defendant FMR LLC is subject to this Court's specific and/or general personal jurisdiction pursuant to due process and/or the Texas Long Arm Statute, due at least to its substantial business in this forum, including: (i) at least a portion of the infringements alleged herein; and/or (ii) regularly doing or soliciting business, engaging in other persistent courses of conduct, and/or deriving substantial revenue from goods and services provided to individuals in Texas and in this Judicial District.

61. On information and belief, Defendant FMR Corp. is subject to this Court's specific and/or general personal jurisdiction pursuant to due process and/or the Texas Long Arm Statute, due at least to its substantial business in this forum, including: (i) at least a portion of the infringements alleged herein; and/or (ii) regularly doing or soliciting business, engaging in other

persistent courses of conduct, and/or deriving substantial revenue from goods and services provided to individuals in Texas and in this Judicial District.

62. On information and belief, Defendant Goldman Sachs is subject to this Court's specific and/or general personal jurisdiction pursuant to due process and/or the Texas Long Arm Statute, due at least to its substantial business in this forum, including: (i) at least a portion of the infringements alleged herein; and/or (ii) regularly doing or soliciting business, engaging in other persistent courses of conduct, and/or deriving substantial revenue from goods and services provided to individuals in Texas and in this Judicial District.

63. On information and belief, Defendant GS & Co. is subject to this Court's specific and/or general personal jurisdiction pursuant to due process and/or the Texas Long Arm Statute, due at least to its substantial business in this forum, including: (i) at least a portion of the infringements alleged herein; and/or (ii) regularly doing or soliciting business, engaging in other persistent courses of conduct, and/or deriving substantial revenue from goods and services provided to individuals in Texas and in this Judicial District.

64. On information and belief, Defendant ING is subject to this Court's specific and/or general personal jurisdiction pursuant to due process and/or the Texas Long Arm Statute, due at least to its substantial business in this forum, including: (i) at least a portion of the infringements alleged herein; and/or (ii) regularly doing or soliciting business, engaging in other persistent courses of conduct, and/or deriving substantial revenue from goods and services provided to individuals in Texas and in this Judicial District.

65. On information and belief, Defendant ING Bank is subject to this Court's specific and/or general personal jurisdiction pursuant to due process and/or the Texas Long Arm Statute, due at least to its substantial business in this forum, including: (i) at least a portion of the

infringements alleged herein; and/or (ii) regularly doing or soliciting business, engaging in other persistent courses of conduct, and/or deriving substantial revenue from goods and services provided to individuals in Texas and in this Judicial District.

66. On information and belief, Defendant ShareBuilder Securities is subject to this Court's specific and/or general personal jurisdiction pursuant to due process and/or the Texas Long Arm Statute, due at least to its substantial business in this forum, including: (i) at least a portion of the infringements alleged herein; and/or (ii) regularly doing or soliciting business, engaging in other persistent courses of conduct, and/or deriving substantial revenue from goods and services provided to individuals in Texas and in this Judicial District.

67. On information and belief, Defendant ShareBuilder is subject to this Court's specific and/or general personal jurisdiction pursuant to due process and/or the Texas Long Arm Statute, due at least to its substantial business in this forum, including: (i) at least a portion of the infringements alleged herein; and/or (ii) regularly doing or soliciting business, engaging in other persistent courses of conduct, and/or deriving substantial revenue from goods and services provided to individuals in Texas and in this Judicial District.

68. On information and belief, Defendant Morgan Stanley is subject to this Court's specific and/or general personal jurisdiction pursuant to due process and/or the Texas Long Arm Statute, due at least to its substantial business in this forum, including: (i) at least a portion of the infringements alleged herein; and/or (ii) regularly doing or soliciting business, engaging in other persistent courses of conduct, and/or deriving substantial revenue from goods and services provided to individuals in Texas and in this Judicial District.

69. On information and belief, Defendant Morgan Stanley Inc. is subject to this Court's specific and/or general personal jurisdiction pursuant to due process and/or the Texas

Long Arm Statute, due at least to its substantial business in this forum, including: (i) at least a portion of the infringements alleged herein; and/or (ii) regularly doing or soliciting business, engaging in other persistent courses of conduct, and/or deriving substantial revenue from goods and services provided to individuals in Texas and in this Judicial District.

70. On information and belief, Defendant RBS is subject to this Court's specific and/or general personal jurisdiction pursuant to due process and/or the Texas Long Arm Statute, due at least to its substantial business in this forum, including: (i) at least a portion of the infringements alleged herein; and/or (ii) regularly doing or soliciting business, engaging in other persistent courses of conduct, and/or deriving substantial revenue from goods and services provided to individuals in Texas and in this Judicial District.

71. On information and belief, Defendant Citizens Financial is subject to this Court's specific and/or general personal jurisdiction pursuant to due process and/or the Texas Long Arm Statute, due at least to its substantial business in this forum, including: (i) at least a portion of the infringements alleged herein; and/or (ii) regularly doing or soliciting business, engaging in other persistent courses of conduct, and/or deriving substantial revenue from goods and services provided to individuals in Texas and in this Judicial District.

72. On information and belief, Defendant RBS Citizens is subject to this Court's specific and/or general personal jurisdiction pursuant to due process and/or the Texas Long Arm Statute, due at least to its substantial business in this forum, including: (i) at least a portion of the infringements alleged herein; and/or (ii) regularly doing or soliciting business, engaging in other persistent courses of conduct, and/or deriving substantial revenue from goods and services provided to individuals in Texas and in this Judicial District.

73. On information and belief, Defendant Chase is subject to this Court's specific and/or general personal jurisdiction pursuant to due process and/or the Texas Long Arm Statute, due at least to its substantial business in this forum, including: (i) at least a portion of the infringements alleged herein; and/or (ii) regularly doing or soliciting business, engaging in other persistent courses of conduct, and/or deriving substantial revenue from goods and services provided to individuals in Texas and in this Judicial District.

74. On information and belief, Defendant Chase Bank is subject to this Court's specific and/or general personal jurisdiction pursuant to due process and/or the Texas Long Arm Statute, due at least to its substantial business in this forum, including: (i) at least a portion of the infringements alleged herein; and/or (ii) regularly doing or soliciting business, engaging in other persistent courses of conduct, and/or deriving substantial revenue from goods and services provided to individuals in Texas and in this Judicial District.

75. On information and belief, Defendant Raymond James is subject to this Court's specific and/or general personal jurisdiction pursuant to due process and/or the Texas Long Arm Statute, due at least to its substantial business in this forum, including: (i) at least a portion of the infringements alleged herein; and/or (ii) regularly doing or soliciting business, engaging in other persistent courses of conduct, and/or deriving substantial revenue from goods and services provided to individuals in Texas and in this Judicial District.

76. On information and belief, Defendant TD AMERITRADE Holding is subject to this Court's specific and/or general personal jurisdiction pursuant to due process and/or the Texas Long Arm Statute, due at least to its substantial business in this forum, including: (i) at least a portion of the infringements alleged herein; and/or (ii) regularly doing or soliciting business,

engaging in other persistent courses of conduct, and/or deriving substantial revenue from goods and services provided to individuals in Texas and in this Judicial District.

77. On information and belief, Defendant TD AMERITRADE is subject to this Court's specific and/or general personal jurisdiction pursuant to due process and/or the Texas Long Arm Statute, due at least to its substantial business in this forum, including: (i) at least a portion of the infringements alleged herein; and/or (ii) regularly doing or soliciting business, engaging in other persistent courses of conduct, and/or deriving substantial revenue from goods and services provided to individuals in Texas and in this Judicial District.

78. On information and belief, Defendant Regions is subject to this Court's specific and/or general personal jurisdiction pursuant to due process and/or the Texas Long Arm Statute, due at least to its substantial business in this forum, including: (i) at least a portion of the infringements alleged herein; and/or (ii) regularly doing or soliciting business, engaging in other persistent courses of conduct, and/or deriving substantial revenue from goods and services provided to individuals in Texas and in this Judicial District.

79. On information and belief, Defendant National City is subject to this Court's specific and/or general personal jurisdiction pursuant to due process and/or the Texas Long Arm Statute, due at least to its substantial business in this forum, including: (i) at least a portion of the infringements alleged herein; and/or (ii) regularly doing or soliciting business, engaging in other persistent courses of conduct, and/or deriving substantial revenue from goods and services provided to individuals in Texas and in this Judicial District.

80. On information and belief, Defendant National City Bank is subject to this Court's specific and/or general personal jurisdiction pursuant to due process and/or the Texas Long Arm Statute, due at least to its substantial business in this forum, including: (i) at least a

portion of the infringements alleged herein; and/or (ii) regularly doing or soliciting business, engaging in other persistent courses of conduct, and/or deriving substantial revenue from goods and services provided to individuals in Texas and in this Judicial District.

81. On information and belief, Defendant IBC is subject to this Court's specific and/or general personal jurisdiction pursuant to due process and/or the Texas Long Arm Statute, due at least to its substantial business in this forum, including: (i) at least a portion of the infringements alleged herein; and/or (ii) regularly doing or soliciting business, engaging in other persistent courses of conduct, and/or deriving substantial revenue from goods and services provided to individuals in Texas and in this Judicial District.

82. On information and belief, Defendant IBC Subsidiary is subject to this Court's specific and/or general personal jurisdiction pursuant to due process and/or the Texas Long Arm Statute, due at least to its substantial business in this forum, including: (i) at least a portion of the infringements alleged herein; and/or (ii) regularly doing or soliciting business, engaging in other persistent courses of conduct, and/or deriving substantial revenue from goods and services provided to individuals in Texas and in this Judicial District.

83. On information and belief, Defendant IBC Bank is subject to this Court's specific and/or general personal jurisdiction pursuant to due process and/or the Texas Long Arm Statute, due at least to its substantial business in this forum, including: (i) at least a portion of the infringements alleged herein; and/or (ii) regularly doing or soliciting business, engaging in other persistent courses of conduct, and/or deriving substantial revenue from goods and services provided to individuals in Texas and in this Judicial District.

84. On information and belief, Defendant Amegy is subject to this Court's specific and/or general personal jurisdiction pursuant to due process and/or the Texas Long Arm Statute,

due at least to its substantial business in this forum, including: (i) at least a portion of the infringements alleged herein; and/or (ii) regularly doing or soliciting business, engaging in other persistent courses of conduct, and/or deriving substantial revenue from goods and services provided to individuals in Texas and in this Judicial District.

85. On information and belief, Defendant Amegy Bank is subject to this Court's specific and/or general personal jurisdiction pursuant to due process and/or the Texas Long Arm Statute, due at least to its substantial business in this forum, including: (i) at least a portion of the infringements alleged herein; and/or (ii) regularly doing or soliciting business, engaging in other persistent courses of conduct, and/or deriving substantial revenue from goods and services provided to individuals in Texas and in this Judicial District.

86. On information and belief, Defendant Fifth Third is subject to this Court's specific and/or general personal jurisdiction pursuant to due process and/or the Texas Long Arm Statute, due at least to its substantial business in this forum, including: (i) at least a portion of the infringements alleged herein; and/or (ii) regularly doing or soliciting business, engaging in other persistent courses of conduct, and/or deriving substantial revenue from goods and services provided to individuals in Texas and in this Judicial District.

87. On information and belief, Defendant Fifth Third Bank is subject to this Court's specific and/or general personal jurisdiction pursuant to due process and/or the Texas Long Arm Statute, due at least to its substantial business in this forum, including: (i) at least a portion of the infringements alleged herein; and/or (ii) regularly doing or soliciting business, engaging in other persistent courses of conduct, and/or deriving substantial revenue from goods and services provided to individuals in Texas and in this Judicial District.

**COUNT I**

**INFRINGEMENT OF U.S. PATENT NO. 5,412,730**

88. Plaintiff is the owner by assignment of United States Patent No. 5,412,730 (“the ‘730 Patent”) entitled “Encrypted Data Transmission System Employing Means for Randomly Altering the Encryption Keys.” The ‘730 Patent issued on May 2, 1995. A true and correct copy of the ‘730 Patent is attached as Exhibit A.

89. Upon information and belief, Defendant Merrill Lynch has been and now is directly and jointly infringing, and indirectly infringing by way of inducing infringement and/or contributing to the infringement of the ‘730 Patent in the State of Texas, in this judicial district, and elsewhere in the United States, by, among other things, methods practiced on various Merrill Lynch websites (including, without limitation, ml.com) for transmitting data comprising a sequence of blocks in encrypted form over a communication link covered by one or more claims of the ‘730 Patent to the injury of TQP. For example, when Merrill Lynch and/or Merrill Lynch’s customers connect to Merrill Lynch’s website, a communication link is established between host servers and the client computer. Data transmitted over this communication link comprises a sequence of blocks, and is transmitted as packets in a sequence over the communication link. Certain data transmissions (both from the client computer to the host server, and from the host server to the client computer) are encrypted according to the claimed method. In order to communicate with encrypted portions of Merrill Lynch’s website, client computers must agree to an encryption algorithm or protocol. Once that protocol is established by the host server, the client computer automatically implements the claimed encryption algorithm under the direction of the host server. Merrill Lynch provides, or directs the client computer to provide, a seed value for both the transmitter and receiver in a symmetric encryption

algorithm, and uses the same key to encrypt and decrypt data. Merrill Lynch generates, or directs the client computer to generate, a first sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at the transmitter (whichever of the host server or client computer is sending the encrypted information), each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link. Merrill Lynch encrypts data for transmission from the host server to the client. In addition, the Merrill Lynch directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. Merrill Lynch generates, or directs the client computer to generate, a second sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at said receiver, each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link such that said first and second sequences are identical to one another, as is used in a symmetric algorithm, a new one of said key values in said first and second sequences being produced each time a predetermined number of said blocks are transmitted over said link. Merrill Lynch decrypts data sent from the client in order to use the data, and directs the client computer to decrypt data transmitted from the host server in order to provide a useable display to, for example, a user of the client computer. Defendant Merrill Lynch is thus liable for infringement of the '730 Patent pursuant to 35 U.S.C. § 271.

90. Upon information and belief, Defendant BOA has been and now is directly and jointly infringing, and indirectly infringing by way of inducing infringement and/or contributing to the infringement of the '730 Patent in the State of Texas, in this judicial district, and elsewhere in the United States, by, among other things, methods practiced on various BOA websites

(including, without limitation, bankofamerica.com) for transmitting data comprising a sequence of blocks in encrypted form over a communication link covered by one or more claims of the '730 Patent to the injury of TQP. For example, when BOA and/or BOA's customers connect to BOA's website, a communication link is established between host servers and the client computer. Data transmitted over this communication link comprises a sequence of blocks, and is transmitted as packets in a sequence over the communication link. Certain data transmissions (both from the client computer to the host server, and from the host server to the client computer) are encrypted according to the claimed method. In order to communicate with encrypted portions of BOA's website, client computers must agree to an encryption algorithm or protocol. Once that protocol is established by the host server, the client computer automatically implements the claimed encryption algorithm under the direction of the host server. BOA provides, or directs the client computer to provide, a seed value for both the transmitter and receiver in a symmetric encryption algorithm, and uses the same key to encrypt and decrypt data. BOA generates, or directs the client computer to generate, a first sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at the transmitter (whichever of the host server or client computer is sending the encrypted information), each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link. BOA encrypts data for transmission from the host server to the client. In addition, the BOA directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. BOA generates, or directs the client computer to generate, a second sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at said receiver, each new key value in said sequence being

produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link such that said first and second sequences are identical to one another, as is used in a symmetric algorithm, a new one of said key values in said first and second sequences being produced each time a predetermined number of said blocks are transmitted over said link. BOA decrypts data sent from the client in order to use the data, and directs the client computer to decrypt data transmitted from the host server in order to provide a useable display to, for example, a user of the client computer. Defendant BOA is thus liable for infringement of the '730 Patent pursuant to 35 U.S.C. § 271.

91. Upon information and belief, Defendant BOA NA has been and now is directly and jointly infringing, and indirectly infringing by way of inducing infringement and/or contributing to the infringement of the '730 Patent in the State of Texas, in this judicial district, and elsewhere in the United States, by, among other things, methods practiced on various BOA NA websites (including, without limitation, bankofamerica.com) for transmitting data comprising a sequence of blocks in encrypted form over a communication link covered by one or more claims of the '730 Patent to the injury of TQP. For example, when BOA NA and/or BOA NA's customers connect to BOA NA's website, a communication link is established between host servers and the client computer. Data transmitted over this communication link comprises a sequence of blocks, and is transmitted as packets in a sequence over the communication link. Certain data transmissions (both from the client computer to the host server, and from the host server to the client computer) are encrypted according to the claimed method. In order to communicate with encrypted portions of BOA NA's website, client computers must agree to an encryption algorithm or protocol. Once that protocol is established by the host server, the client computer automatically implements the claimed encryption algorithm under the direction of the

host server. BOA NA provides, or directs the client computer to provide, a seed value for both the transmitter and receiver in a symmetric encryption algorithm, and uses the same key to encrypt and decrypt data. BOA NA generates, or directs the client computer to generate, a first sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at the transmitter (whichever of the host server or client computer is sending the encrypted information), each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link. BOA NA encrypts data for transmission from the host server to the client. In addition, the BOA NA directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. BOA NA generates, or directs the client computer to generate, a second sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at said receiver, each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link such that said first and second sequences are identical to one another, as is used in a symmetric algorithm, a new one of said key values in said first and second sequences being produced each time a predetermined number of said blocks are transmitted over said link. BOA NA decrypts data sent from the client in order to use the data, and directs the client computer to decrypt data transmitted from the host server in order to provide a useable display to, for example, a user of the client computer. Defendant BOA NA is thus liable for infringement of the '730 Patent pursuant to 35 U.S.C. § 271.

92. Upon information and belief, Defendant Capital has been and now is directly and jointly infringing, and indirectly infringing by way of inducing infringement and/or contributing to the infringement of the '730 Patent in the State of Texas, in this judicial district, and elsewhere

in the United States, by, among other things, methods practiced on various Capital websites (including, without limitation, [capitalone.com](http://capitalone.com)) for transmitting data comprising a sequence of blocks in encrypted form over a communication link covered by one or more claims of the '730 Patent to the injury of TQP. For example, when Capital and/or Capital's customers connect to Capital's website, a communication link is established between host servers and the client computer. Data transmitted over this communication link comprises a sequence of blocks, and is transmitted as packets in a sequence over the communication link. Certain data transmissions (both from the client computer to the host server, and from the host server to the client computer) are encrypted according to the claimed method. In order to communicate with encrypted portions of Capital's website, client computers must agree to an encryption algorithm or protocol. Once that protocol is established by the host server, the client computer automatically implements the claimed encryption algorithm under the direction of the host server. Capital provides, or directs the client computer to provide, a seed value for both the transmitter and receiver in a symmetric encryption algorithm, and uses the same key to encrypt and decrypt data. Capital generates, or directs the client computer to generate, a first sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at the transmitter (whichever of the host server or client computer is sending the encrypted information), each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link. Capital encrypts data for transmission from the host server to the client. In addition, the Capital directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. Capital generates, or directs the client computer to generate, a second sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt

data, based on said seed value at said receiver, each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link such that said first and second sequences are identical to one another, as is used in a symmetric algorithm, a new one of said key values in said first and second sequences being produced each time a predetermined number of said blocks are transmitted over said link. Capital decrypts data sent from the client in order to use the data, and directs the client computer to decrypt data transmitted from the host server in order to provide a useable display to, for example, a user of the client computer. Defendant Capital is thus liable for infringement of the '730 Patent pursuant to 35 U.S.C. § 271.

93. Upon information and belief, Defendant Capital One has been and now is directly and jointly infringing, and indirectly infringing by way of inducing infringement and/or contributing to the infringement of the '730 Patent in the State of Texas, in this judicial district, and elsewhere in the United States, by, among other things, methods practiced on various Capital One websites (including, without limitation, [capitalone.com](http://capitalone.com)) for transmitting data comprising a sequence of blocks in encrypted form over a communication link covered by one or more claims of the '730 Patent to the injury of TQP. For example, when Capital One and/or Capital One's customers connect to Capital One's website, a communication link is established between host servers and the client computer. Data transmitted over this communication link comprises a sequence of blocks, and is transmitted as packets in a sequence over the communication link. Certain data transmissions (both from the client computer to the host server, and from the host server to the client computer) are encrypted according to the claimed method. In order to communicate with encrypted portions of Capital One's website, client computers must agree to an encryption algorithm or protocol. Once that protocol is established

by the host server, the client computer automatically implements the claimed encryption algorithm under the direction of the host server. Capital One provides, or directs the client computer to provide, a seed value for both the transmitter and receiver in a symmetric encryption algorithm, and uses the same key to encrypt and decrypt data. Capital One generates, or directs the client computer to generate, a first sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at the transmitter (whichever of the host server or client computer is sending the encrypted information), each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link. Capital One encrypts data for transmission from the host server to the client. In addition, the Capital One directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. Capital One generates, or directs the client computer to generate, a second sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at said receiver, each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link such that said first and second sequences are identical to one another, as is used in a symmetric algorithm, a new one of said key values in said first and second sequences being produced each time a predetermined number of said blocks are transmitted over said link. Capital One decrypts data sent from the client in order to use the data, and directs the client computer to decrypt data transmitted from the host server in order to provide a useable display to, for example, a user of the client computer. Defendant Capital One is thus liable for infringement of the '730 Patent pursuant to 35 U.S.C. § 271.

94. Upon information and belief, Defendant Capital One NA has been and now is directly and jointly infringing, and indirectly infringing by way of inducing infringement and/or contributing to the infringement of the '730 Patent in the State of Texas, in this judicial district, and elsewhere in the United States, by, among other things, methods practiced on various Capital One NA websites (including, without limitation, [capitalone.com](http://capitalone.com)) for transmitting data comprising a sequence of blocks in encrypted form over a communication link covered by one or more claims of the '730 Patent to the injury of TQP. For example, when Capital One NA and/or Capital One NA's customers connect to Capital One NA's website, a communication link is established between host servers and the client computer. Data transmitted over this communication link comprises a sequence of blocks, and is transmitted as packets in a sequence over the communication link. Certain data transmissions (both from the client computer to the host server, and from the host server to the client computer) are encrypted according to the claimed method. In order to communicate with encrypted portions of Capital One NA's website, client computers must agree to an encryption algorithm or protocol. Once that protocol is established by the host server, the client computer automatically implements the claimed encryption algorithm under the direction of the host server. Capital One NA provides, or directs the client computer to provide, a seed value for both the transmitter and receiver in a symmetric encryption algorithm, and uses the same key to encrypt and decrypt data. Capital One NA generates, or directs the client computer to generate, a first sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at the transmitter (whichever of the host server or client computer is sending the encrypted information), each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link. Capital One NA

encrypts data for transmission from the host server to the client. In addition, the Capital One NA directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. Capital One NA generates, or directs the client computer to generate, a second sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at said receiver, each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link such that said first and second sequences are identical to one another, as is used in a symmetric algorithm, a new one of said key values in said first and second sequences being produced each time a predetermined number of said blocks are transmitted over said link. Capital One NA decrypts data sent from the client in order to use the data, and directs the client computer to decrypt data transmitted from the host server in order to provide a useable display to, for example, a user of the client computer. Defendant Capital One NA is thus liable for infringement of the '730 Patent pursuant to 35 U.S.C. § 271.

95. Upon information and belief, Defendant Comerica has been and now is directly and jointly infringing, and indirectly infringing by way of inducing infringement and/or contributing to the infringement of the '730 Patent in the State of Texas, in this judicial district, and elsewhere in the United States, by, among other things, methods practiced on various Comerica websites (including, without limitation, [comerica.com](http://comerica.com)) for transmitting data comprising a sequence of blocks in encrypted form over a communication link covered by one or more claims of the '730 Patent to the injury of TQP. For example, when Comerica and/or Comerica's customers connect to Comerica's website, a communication link is established between host servers and the client computer. Data transmitted over this communication link comprises a sequence of blocks, and is transmitted as packets in a sequence over the

communication link. Certain data transmissions (both from the client computer to the host server, and from the host server to the client computer) are encrypted according to the claimed method. In order to communicate with encrypted portions of Comerica's website, client computers must agree to an encryption algorithm or protocol. Once that protocol is established by the host server, the client computer automatically implements the claimed encryption algorithm under the direction of the host server. Comerica provides, or directs the client computer to provide, a seed value for both the transmitter and receiver in a symmetric encryption algorithm, and uses the same key to encrypt and decrypt data. Comerica generates, or directs the client computer to generate, a first sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at the transmitter (whichever of the host server or client computer is sending the encrypted information), each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link. Comerica encrypts data for transmission from the host server to the client. In addition, the Comerica directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. Comerica generates, or directs the client computer to generate, a second sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at said receiver, each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link such that said first and second sequences are identical to one another, as is used in a symmetric algorithm, a new one of said key values in said first and second sequences being produced each time a predetermined number of said blocks are transmitted over said link. Comerica decrypts data sent from the client in order to use the data, and directs the client computer to decrypt data

transmitted from the host server in order to provide a useable display to, for example, a user of the client computer. Defendant Comerica is thus liable for infringement of the '730 Patent pursuant to 35 U.S.C. § 271.

96. Upon information and belief, Defendant Comerica Bank has been and now is directly and jointly infringing, and indirectly infringing by way of inducing infringement and/or contributing to the infringement of the '730 Patent in the State of Texas, in this judicial district, and elsewhere in the United States, by, among other things, methods practiced on various Comerica Bank websites (including, without limitation, comerica.com) for transmitting data comprising a sequence of blocks in encrypted form over a communication link covered by one or more claims of the '730 Patent to the injury of TQP. For example, when Comerica Bank and/or Comerica Bank's customers connect to Comerica Bank's website, a communication link is established between host servers and the client computer. Data transmitted over this communication link comprises a sequence of blocks, and is transmitted as packets in a sequence over the communication link. Certain data transmissions (both from the client computer to the host server, and from the host server to the client computer) are encrypted according to the claimed method. In order to communicate with encrypted portions of Comerica Bank's website, client computers must agree to an encryption algorithm or protocol. Once that protocol is established by the host server, the client computer automatically implements the claimed encryption algorithm under the direction of the host server. Comerica Bank provides, or directs the client computer to provide, a seed value for both the transmitter and receiver in a symmetric encryption algorithm, and uses the same key to encrypt and decrypt data. Comerica Bank generates, or directs the client computer to generate, a first sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at

the transmitter (whichever of the host server or client computer is sending the encrypted information), each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link. Comerica Bank encrypts data for transmission from the host server to the client. In addition, the Comerica Bank directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. Comerica Bank generates, or directs the client computer to generate, a second sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at said receiver, each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link such that said first and second sequences are identical to one another, as is used in a symmetric algorithm, a new one of said key values in said first and second sequences being produced each time a predetermined number of said blocks are transmitted over said link. Comerica Bank decrypts data sent from the client in order to use the data, and directs the client computer to decrypt data transmitted from the host server in order to provide a useable display to, for example, a user of the client computer. Defendant Comerica Bank is thus liable for infringement of the '730 Patent pursuant to 35 U.S.C. § 271.

97. Upon information and belief, Defendant Citigroup has been and now is directly and jointly infringing, and indirectly infringing by way of inducing infringement and/or contributing to the infringement of the '730 Patent in the State of Texas, in this judicial district, and elsewhere in the United States, by, among other things, methods practiced on various Citigroup websites (including, without limitation domains residing at, citibank.com, primerica.impress-net.com, and smithbarney.com) for transmitting data comprising a sequence of blocks in encrypted form over a communication link covered by one or more claims of the

'730 Patent to the injury of TQP. For example, when Citigroup and/or Citigroup's customers connect to Citigroup's website, a communication link is established between host servers and the client computer. Data transmitted over this communication link comprises a sequence of blocks, and is transmitted as packets in a sequence over the communication link. Certain data transmissions (both from the client computer to the host server, and from the host server to the client computer) are encrypted according to the claimed method. In order to communicate with encrypted portions of Citigroup's website, client computers must agree to an encryption algorithm or protocol. Once that protocol is established by the host server, the client computer automatically implements the claimed encryption algorithm under the direction of the host server. Citigroup provides, or directs the client computer to provide, a seed value for both the transmitter and receiver in a symmetric encryption algorithm, and uses the same key to encrypt and decrypt data. Citigroup generates, or directs the client computer to generate, a first sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at the transmitter (whichever of the host server or client computer is sending the encrypted information), each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link. Citigroup encrypts data for transmission from the host server to the client. In addition, the Citigroup directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. Citigroup generates, or directs the client computer to generate, a second sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at said receiver, each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link such that said first and second sequences are identical

to one another, as is used in a symmetric algorithm, a new one of said key values in said first and second sequences being produced each time a predetermined number of said blocks are transmitted over said link. Citigroup decrypts data sent from the client in order to use the data, and directs the client computer to decrypt data transmitted from the host server in order to provide a useable display to, for example, a user of the client computer. Defendant Citigroup is thus liable for infringement of the '730 Patent pursuant to 35 U.S.C. § 271.

98. Upon information and belief, Defendant Primerica has been and now is directly and jointly infringing, and indirectly infringing by way of inducing infringement and/or contributing to the infringement of the '730 Patent in the State of Texas, in this judicial district, and elsewhere in the United States, by, among other things, methods practiced on various Primerica websites (including, without limitation domains residing at, primerica.impress-net.com) for transmitting data comprising a sequence of blocks in encrypted form over a communication link covered by one or more claims of the '730 Patent to the injury of TQP. For example, when Primerica and/or Primerica's customers connect to Primerica's website, a communication link is established between host servers and the client computer. Data transmitted over this communication link comprises a sequence of blocks, and is transmitted as packets in a sequence over the communication link. Certain data transmissions (both from the client computer to the host server, and from the host server to the client computer) are encrypted according to the claimed method. In order to communicate with encrypted portions of Primerica's website, client computers must agree to an encryption algorithm or protocol. Once that protocol is established by the host server, the client computer automatically implements the claimed encryption algorithm under the direction of the host server. Primerica provides, or directs the client computer to provide, a seed value for both the transmitter and receiver in a

symmetric encryption algorithm, and uses the same key to encrypt and decrypt data. Primerica generates, or directs the client computer to generate, a first sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at the transmitter (whichever of the host server or client computer is sending the encrypted information), each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link. Primerica encrypts data for transmission from the host server to the client. In addition, the Primerica directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. Primerica generates, or directs the client computer to generate, a second sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at said receiver, each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link such that said first and second sequences are identical to one another, as is used in a symmetric algorithm, a new one of said key values in said first and second sequences being produced each time a predetermined number of said blocks are transmitted over said link. Primerica decrypts data sent from the client in order to use the data, and directs the client computer to decrypt data transmitted from the host server in order to provide a useable display to, for example, a user of the client computer. Defendant Primerica is thus liable for infringement of the '730 Patent pursuant to 35 U.S.C. § 271.

99. Upon information and belief, Defendant Citibank has been and now is directly and jointly infringing, and indirectly infringing by way of inducing infringement and/or contributing to the infringement of the '730 Patent in the State of Texas, in this judicial district, and elsewhere in the United States, by, among other things, methods practiced on various

Citibank websites (including, without limitation, citibank.com and smithbarney.com) for transmitting data comprising a sequence of blocks in encrypted form over a communication link covered by one or more claims of the '730 Patent to the injury of TQP. For example, when Citibank and/or Citibank's customers connect to Citibank's website, a communication link is established between host servers and the client computer. Data transmitted over this communication link comprises a sequence of blocks, and is transmitted as packets in a sequence over the communication link. Certain data transmissions (both from the client computer to the host server, and from the host server to the client computer) are encrypted according to the claimed method. In order to communicate with encrypted portions of Citibank's website, client computers must agree to an encryption algorithm or protocol. Once that protocol is established by the host server, the client computer automatically implements the claimed encryption algorithm under the direction of the host server. Citibank provides, or directs the client computer to provide, a seed value for both the transmitter and receiver in a symmetric encryption algorithm, and uses the same key to encrypt and decrypt data. Citibank generates, or directs the client computer to generate, a first sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at the transmitter (whichever of the host server or client computer is sending the encrypted information), each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link. Citibank encrypts data for transmission from the host server to the client. In addition, the Citibank directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. Citibank generates, or directs the client computer to generate, a second sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on

said seed value at said receiver, each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link such that said first and second sequences are identical to one another, as is used in a symmetric algorithm, a new one of said key values in said first and second sequences being produced each time a predetermined number of said blocks are transmitted over said link. Citibank decrypts data sent from the client in order to use the data, and directs the client computer to decrypt data transmitted from the host server in order to provide a useable display to, for example, a user of the client computer. Defendant Citibank is thus liable for infringement of the '730 Patent pursuant to 35 U.S.C. § 271.

100. Upon information and belief, Defendant Smith Barney has been and now is directly and jointly infringing, and indirectly infringing by way of inducing infringement and/or contributing to the infringement of the '730 Patent in the State of Texas, in this judicial district, and elsewhere in the United States, by, among other things, methods practiced on various Smith Barney websites (including, without limitation, smithbarney.com) for transmitting data comprising a sequence of blocks in encrypted form over a communication link covered by one or more claims of the '730 Patent to the injury of TQP. For example, when Smith Barney and/or Smith Barney's customers connect to Smith Barney's website, a communication link is established between host servers and the client computer. Data transmitted over this communication link comprises a sequence of blocks, and is transmitted as packets in a sequence over the communication link. Certain data transmissions (both from the client computer to the host server, and from the host server to the client computer) are encrypted according to the claimed method. In order to communicate with encrypted portions of Smith Barney's website, client computers must agree to an encryption algorithm or protocol. Once that protocol is

established by the host server, the client computer automatically implements the claimed encryption algorithm under the direction of the host server. Smith Barney provides, or directs the client computer to provide, a seed value for both the transmitter and receiver in a symmetric encryption algorithm, and uses the same key to encrypt and decrypt data. Smith Barney generates, or directs the client computer to generate, a first sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at the transmitter (whichever of the host server or client computer is sending the encrypted information), each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link. Smith Barney encrypts data for transmission from the host server to the client. In addition, the Smith Barney directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. Smith Barney generates, or directs the client computer to generate, a second sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at said receiver, each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link such that said first and second sequences are identical to one another, as is used in a symmetric algorithm, a new one of said key values in said first and second sequences being produced each time a predetermined number of said blocks are transmitted over said link. Smith Barney decrypts data sent from the client in order to use the data, and directs the client computer to decrypt data transmitted from the host server in order to provide a useable display to, for example, a user of the client computer. Defendant Smith Barney is thus liable for infringement of the '730 Patent pursuant to 35 U.S.C. § 271.

101. Upon information and belief, Defendant E\*Trade has been and now is directly and jointly infringing, and indirectly infringing by way of inducing infringement and/or contributing to the infringement of the '730 Patent in the State of Texas, in this judicial district, and elsewhere in the United States, by, among other things, methods practiced on various E\*Trade websites (including, without limitation, etrade.com) for transmitting data comprising a sequence of blocks in encrypted form over a communication link covered by one or more claims of the '730 Patent to the injury of TQP. For example, when E\*Trade and/or E\*Trade's customers connect to E\*Trade's website, a communication link is established between host servers and the client computer. Data transmitted over this communication link comprises a sequence of blocks, and is transmitted as packets in a sequence over the communication link. Certain data transmissions (both from the client computer to the host server, and from the host server to the client computer) are encrypted according to the claimed method. In order to communicate with encrypted portions of E\*Trade's website, client computers must agree to an encryption algorithm or protocol. Once that protocol is established by the host server, the client computer automatically implements the claimed encryption algorithm under the direction of the host server. E\*Trade provides, or directs the client computer to provide, a seed value for both the transmitter and receiver in a symmetric encryption algorithm, and uses the same key to encrypt and decrypt data. E\*Trade generates, or directs the client computer to generate, a first sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at the transmitter (whichever of the host server or client computer is sending the encrypted information), each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link. E\*Trade encrypts data for transmission from the host server to the client. In addition, the

E\*Trade directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. E\*Trade generates, or directs the client computer to generate, a second sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at said receiver, each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link such that said first and second sequences are identical to one another, as is used in a symmetric algorithm, a new one of said key values in said first and second sequences being produced each time a predetermined number of said blocks are transmitted over said link. E\*Trade decrypts data sent from the client in order to use the data, and directs the client computer to decrypt data transmitted from the host server in order to provide a useable display to, for example, a user of the client computer. Defendant E\*Trade is thus liable for infringement of the '730 Patent pursuant to 35 U.S.C. § 271.

102. Upon information and belief, Defendant Fidelity has been and now is directly and jointly infringing, and indirectly infringing by way of inducing infringement and/or contributing to the infringement of the '730 Patent in the State of Texas, in this judicial district, and elsewhere in the United States, by, among other things, methods practiced on various Fidelity websites (including, without limitation, fidelity.com) for transmitting data comprising a sequence of blocks in encrypted form over a communication link covered by one or more claims of the '730 Patent to the injury of TQP. For example, when Fidelity and/or Fidelity's customers connect to Fidelity's website, a communication link is established between host servers and the client computer. Data transmitted over this communication link comprises a sequence of blocks, and is transmitted as packets in a sequence over the communication link. Certain data transmissions (both from the client computer to the host server, and from the host server to the client computer)

are encrypted according to the claimed method. In order to communicate with encrypted portions of Fidelity's website, client computers must agree to an encryption algorithm or protocol. Once that protocol is established by the host server, the client computer automatically implements the claimed encryption algorithm under the direction of the host server. Fidelity provides, or directs the client computer to provide, a seed value for both the transmitter and receiver in a symmetric encryption algorithm, and uses the same key to encrypt and decrypt data. Fidelity generates, or directs the client computer to generate, a first sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at the transmitter (whichever of the host server or client computer is sending the encrypted information), each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link. Fidelity encrypts data for transmission from the host server to the client. In addition, the Fidelity directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. Fidelity generates, or directs the client computer to generate, a second sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at said receiver, each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link such that said first and second sequences are identical to one another, as is used in a symmetric algorithm, a new one of said key values in said first and second sequences being produced each time a predetermined number of said blocks are transmitted over said link. Fidelity decrypts data sent from the client in order to use the data, and directs the client computer to decrypt data transmitted from the host server in order to provide a useable

display to, for example, a user of the client computer. Defendant Fidelity is thus liable for infringement of the '730 Patent pursuant to 35 U.S.C. § 271.

103. Upon information and belief, Defendant FMR LLC has been and now is directly and jointly infringing, and indirectly infringing by way of inducing infringement and/or contributing to the infringement of the '730 Patent in the State of Texas, in this judicial district, and elsewhere in the United States, by, among other things, methods practiced on various FMR LLC websites (including, without limitation, fidelity.com) for transmitting data comprising a sequence of blocks in encrypted form over a communication link covered by one or more claims of the '730 Patent to the injury of TQP. For example, when FMR LLC and/or FMR LLC's customers connect to FMR LLC's website, a communication link is established between host servers and the client computer. Data transmitted over this communication link comprises a sequence of blocks, and is transmitted as packets in a sequence over the communication link. Certain data transmissions (both from the client computer to the host server, and from the host server to the client computer) are encrypted according to the claimed method. In order to communicate with encrypted portions of FMR LLC's website, client computers must agree to an encryption algorithm or protocol. Once that protocol is established by the host server, the client computer automatically implements the claimed encryption algorithm under the direction of the host server. FMR LLC provides, or directs the client computer to provide, a seed value for both the transmitter and receiver in a symmetric encryption algorithm, and uses the same key to encrypt and decrypt data. FMR LLC generates, or directs the client computer to generate, a first sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at the transmitter (whichever of the host server or client computer is sending the encrypted information), each new key value in said sequence being produced at a

time dependent upon a predetermined characteristic of the data being transmitted over said link. FMR LLC encrypts data for transmission from the host server to the client. In addition, the FMR LLC directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. FMR LLC generates, or directs the client computer to generate, a second sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at said receiver, each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link such that said first and second sequences are identical to one another, as is used in a symmetric algorithm, a new one of said key values in said first and second sequences being produced each time a predetermined number of said blocks are transmitted over said link. FMR LLC decrypts data sent from the client in order to use the data, and directs the client computer to decrypt data transmitted from the host server in order to provide a useable display to, for example, a user of the client computer. Defendant FMR LLC is thus liable for infringement of the '730 Patent pursuant to 35 U.S.C. § 271.

104. Upon information and belief, Defendant FMR Corp. has been and now is directly and jointly infringing, and indirectly infringing by way of inducing infringement and/or contributing to the infringement of the '730 Patent in the State of Texas, in this judicial district, and elsewhere in the United States, by, among other things, methods practiced on various FMR Corp. websites (including, without limitation, fidelity.com) for transmitting data comprising a sequence of blocks in encrypted form over a communication link covered by one or more claims of the '730 Patent to the injury of TQP. For example, when FMR Corp. and/or FMR Corp.'s customers connect to FMR Corp.'s website, a communication link is established between host servers and the client computer. Data transmitted over this communication link comprises a

sequence of blocks, and is transmitted as packets in a sequence over the communication link. Certain data transmissions (both from the client computer to the host server, and from the host server to the client computer) are encrypted according to the claimed method. In order to communicate with encrypted portions of FMR Corp.'s website, client computers must agree to an encryption algorithm or protocol. Once that protocol is established by the host server, the client computer automatically implements the claimed encryption algorithm under the direction of the host server. FMR Corp. provides, or directs the client computer to provide, a seed value for both the transmitter and receiver in a symmetric encryption algorithm, and uses the same key to encrypt and decrypt data. FMR Corp. generates, or directs the client computer to generate, a first sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at the transmitter (whichever of the host server or client computer is sending the encrypted information), each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link. FMR Corp. encrypts data for transmission from the host server to the client. In addition, the FMR Corp. directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. FMR Corp. generates, or directs the client computer to generate, a second sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at said receiver, each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link such that said first and second sequences are identical to one another, as is used in a symmetric algorithm, a new one of said key values in said first and second sequences being produced each time a predetermined number of said blocks are transmitted over said link. FMR Corp. decrypts data sent from the client in

order to use the data, and directs the client computer to decrypt data transmitted from the host server in order to provide a useable display to, for example, a user of the client computer. Defendant FMR Corp. is thus liable for infringement of the '730 Patent pursuant to 35 U.S.C. § 271.

105. Upon information and belief, Defendant Goldman Sachs has been and now is directly and jointly infringing, and indirectly infringing by way of inducing infringement and/or contributing to the infringement of the '730 Patent in the State of Texas, in this judicial district, and elsewhere in the United States, by, among other things, methods practiced on various Goldman Sachs websites (including, without limitation, gs.com, gsfundadmin.com, and goldman.com) for transmitting data comprising a sequence of blocks in encrypted form over a communication link covered by one or more claims of the '730 Patent to the injury of TQP. For example, when Goldman Sachs and/or Goldman Sachs' customers connect to Goldman Sachs' website, a communication link is established between host servers and the client computer. Data transmitted over this communication link comprises a sequence of blocks, and is transmitted as packets in a sequence over the communication link. Certain data transmissions (both from the client computer to the host server, and from the host server to the client computer) are encrypted according to the claimed method. In order to communicate with encrypted portions of Goldman Sachs' website, client computers must agree to an encryption algorithm or protocol. Once that protocol is established by the host server, the client computer automatically implements the claimed encryption algorithm under the direction of the host server. Goldman Sachs provides, or directs the client computer to provide, a seed value for both the transmitter and receiver in a symmetric encryption algorithm, and uses the same key to encrypt and decrypt data. Goldman Sachs generates, or directs the client computer to generate, a first sequence of pseudo-random

key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at the transmitter (whichever of the host server or client computer is sending the encrypted information), each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link. Goldman Sachs encrypts data for transmission from the host server to the client. In addition, the Goldman Sachs directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. Goldman Sachs generates, or directs the client computer to generate, a second sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at said receiver, each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link such that said first and second sequences are identical to one another, as is used in a symmetric algorithm, a new one of said key values in said first and second sequences being produced each time a predetermined number of said blocks are transmitted over said link. Goldman Sachs decrypts data sent from the client in order to use the data, and directs the client computer to decrypt data transmitted from the host server in order to provide a useable display to, for example, a user of the client computer. Defendant Goldman Sachs is thus liable for infringement of the '730 Patent pursuant to 35 U.S.C. § 271.

106. Upon information and belief, Defendant GS & Co. has been and now is directly and jointly infringing, and indirectly infringing by way of inducing infringement and/or contributing to the infringement of the '730 Patent in the State of Texas, in this judicial district, and elsewhere in the United States, by, among other things, methods practiced on various GS & Co. websites (including, without limitation, gs.com, gsfundadmin.com, and goldman.com) for transmitting data comprising a sequence of blocks in encrypted form over a communication link

covered by one or more claims of the '730 Patent to the injury of TQP. For example, when GS & Co. and/or GS & Co.'s customers connect to GS & Co.'s website, a communication link is established between host servers and the client computer. Data transmitted over this communication link comprises a sequence of blocks, and is transmitted as packets in a sequence over the communication link. Certain data transmissions (both from the client computer to the host server, and from the host server to the client computer) are encrypted according to the claimed method. In order to communicate with encrypted portions of GS & Co.'s website, client computers must agree to an encryption algorithm or protocol. Once that protocol is established by the host server, the client computer automatically implements the claimed encryption algorithm under the direction of the host server. GS & Co. provides, or directs the client computer to provide, a seed value for both the transmitter and receiver in a symmetric encryption algorithm, and uses the same key to encrypt and decrypt data. GS & Co. generates, or directs the client computer to generate, a first sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at the transmitter (whichever of the host server or client computer is sending the encrypted information), each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link. GS & Co. encrypts data for transmission from the host server to the client. In addition, the GS & Co. directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. GS & Co. generates, or directs the client computer to generate, a second sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at said receiver, each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link such

that said first and second sequences are identical to one another, as is used in a symmetric algorithm, a new one of said key values in said first and second sequences being produced each time a predetermined number of said blocks are transmitted over said link. GS & Co. decrypts data sent from the client in order to use the data, and directs the client computer to decrypt data transmitted from the host server in order to provide a useable display to, for example, a user of the client computer. Defendant GS & Co. is thus liable for infringement of the '730 Patent pursuant to 35 U.S.C. § 271.

107. Upon information and belief, Defendant ING has been and now is directly and jointly infringing, and indirectly infringing by way of inducing infringement and/or contributing to the infringement of the '730 Patent in the State of Texas, in this judicial district, and elsewhere in the United States, by, among other things, methods practiced on various ING websites (including, without limitation, [ingdirect.com](http://ingdirect.com) and [sharebuilder.com](http://sharebuilder.com)) for transmitting data comprising a sequence of blocks in encrypted form over a communication link covered by one or more claims of the '730 Patent to the injury of TQP. For example, when ING's customers connect to ING's website, a communication link is established between host servers and the client computer. Data transmitted over this communication link comprises a sequence of blocks, and is transmitted as packets in a sequence over the communication link. Certain data transmissions (both from the client computer to the host server, and from the host server to the client computer) are encrypted according to the claimed method. In order to communicate with encrypted portions of ING's website, client computers must agree to an encryption algorithm or protocol. Once that protocol is established by the host server, the client computer automatically implements the claimed encryption algorithm under the direction of the host server. ING provides, or directs the client computer to provide, a seed value for both the transmitter and

receiver in a symmetric encryption algorithm, and uses the same key to encrypt and decrypt data. ING generates, or directs the client computer to generate, a first sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at the transmitter (whichever of the host server or client computer is sending the encrypted information), each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link. ING encrypts data for transmission from the host server to the client. In addition, the ING directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. ING generates, or directs the client computer to generate, a second sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at said receiver, each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link such that said first and second sequences are identical to one another, as is used in a symmetric algorithm, a new one of said key values in said first and second sequences being produced each time a predetermined number of said blocks are transmitted over said link. ING decrypts data sent from the client in order to use the data, and directs the client computer to decrypt data transmitted from the host server in order to provide a useable display to, for example, a user of the client computer. Defendant ING is thus liable for infringement of the '730 Patent pursuant to 35 U.S.C. § 271.

108. Upon information and belief, Defendant ING Bank has been and now is directly and jointly infringing, and indirectly infringing by way of inducing infringement and/or contributing to the infringement of the '730 Patent in the State of Texas, in this judicial district, and elsewhere in the United States, by, among other things, methods practiced on various ING

Bank websites (including, without limitation, [ingdirect.com](http://ingdirect.com) and [sharebuilder.com](http://sharebuilder.com)) for transmitting data comprising a sequence of blocks in encrypted form over a communication link covered by one or more claims of the '730 Patent to the injury of TQP. For example, when ING Bank's customers connect to ING Bank's website, a communication link is established between host servers and the client computer. Data transmitted over this communication link comprises a sequence of blocks, and is transmitted as packets in a sequence over the communication link. Certain data transmissions (both from the client computer to the host server, and from the host server to the client computer) are encrypted according to the claimed method. In order to communicate with encrypted portions of ING Bank's website, client computers must agree to an encryption algorithm or protocol. Once that protocol is established by the host server, the client computer automatically implements the claimed encryption algorithm under the direction of the host server. ING Bank provides, or directs the client computer to provide, a seed value for both the transmitter and receiver in a symmetric encryption algorithm, and uses the same key to encrypt and decrypt data. ING Bank generates, or directs the client computer to generate, a first sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at the transmitter (whichever of the host server or client computer is sending the encrypted information), each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link. ING Bank encrypts data for transmission from the host server to the client. In addition, the ING Bank directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. ING Bank generates, or directs the client computer to generate, a second sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at said receiver, each new key

value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link such that said first and second sequences are identical to one another, as is used in a symmetric algorithm, a new one of said key values in said first and second sequences being produced each time a predetermined number of said blocks are transmitted over said link. ING Bank decrypts data sent from the client in order to use the data, and directs the client computer to decrypt data transmitted from the host server in order to provide a useable display to, for example, a user of the client computer. Defendant ING Bank is thus liable for infringement of the '730 Patent pursuant to 35 U.S.C. § 271.

109. Upon information and belief, Defendant Sharebuilder Securities has been and now is directly and jointly infringing, and indirectly infringing by way of inducing infringement and/or contributing to the infringement of the '730 Patent in the State of Texas, in this judicial district, and elsewhere in the United States, by, among other things, methods practiced on various Sharebuilder Securities websites (including, without limitation, sharebuilder.com) for transmitting data comprising a sequence of blocks in encrypted form over a communication link covered by one or more claims of the '730 Patent to the injury of TQP. For example, when Sharebuilder Securities' customers connect to Sharebuilder Securities' website, a communication link is established between host servers and the client computer. Data transmitted over this communication link comprises a sequence of blocks, and is transmitted as packets in a sequence over the communication link. Certain data transmissions (both from the client computer to the host server, and from the host server to the client computer) are encrypted according to the claimed method. In order to communicate with encrypted portions of Sharebuilder Securities' website, client computers must agree to an encryption algorithm or protocol. Once that protocol is established by the host server, the client computer automatically implements the claimed

encryption algorithm under the direction of the host server. Sharebuilder Securities provides, or directs the client computer to provide, a seed value for both the transmitter and receiver in a symmetric encryption algorithm, and uses the same key to encrypt and decrypt data. Sharebuilder Securities generates, or directs the client computer to generate, a first sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at the transmitter (whichever of the host server or client computer is sending the encrypted information), each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link. Sharebuilder Securities encrypts data for transmission from the host server to the client. In addition, the Sharebuilder Securities directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. Sharebuilder Securities generates, or directs the client computer to generate, a second sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at said receiver, each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link such that said first and second sequences are identical to one another, as is used in a symmetric algorithm, a new one of said key values in said first and second sequences being produced each time a predetermined number of said blocks are transmitted over said link. Sharebuilder Securities decrypts data sent from the client in order to use the data, and directs the client computer to decrypt data transmitted from the host server in order to provide a useable display to, for example, a user of the client computer. Defendant Sharebuilder Securities is thus liable for infringement of the '730 Patent pursuant to 35 U.S.C. § 271.

110. Upon information and belief, Defendant Sharebuilder has been and now is directly and jointly infringing, and indirectly infringing by way of inducing infringement and/or contributing to the infringement of the '730 Patent in the State of Texas, in this judicial district, and elsewhere in the United States, by, among other things, methods practiced on various Sharebuilder websites (including, without limitation, sharebuilder.com) for transmitting data comprising a sequence of blocks in encrypted form over a communication link covered by one or more claims of the '730 Patent to the injury of TQP. For example, when Sharebuilder's customers connect to Sharebuilder's website, a communication link is established between host servers and the client computer. Data transmitted over this communication link comprises a sequence of blocks, and is transmitted as packets in a sequence over the communication link. Certain data transmissions (both from the client computer to the host server, and from the host server to the client computer) are encrypted according to the claimed method. In order to communicate with encrypted portions of Sharebuilder's website, client computers must agree to an encryption algorithm or protocol. Once that protocol is established by the host server, the client computer automatically implements the claimed encryption algorithm under the direction of the host server. Sharebuilder provides, or directs the client computer to provide, a seed value for both the transmitter and receiver in a symmetric encryption algorithm, and uses the same key to encrypt and decrypt data. Sharebuilder generates, or directs the client computer to generate, a first sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at the transmitter (whichever of the host server or client computer is sending the encrypted information), each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link. Sharebuilder encrypts data for transmission from the host server to the client. In

addition, the Sharebuilder directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. Sharebuilder generates, or directs the client computer to generate, a second sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at said receiver, each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link such that said first and second sequences are identical to one another, as is used in a symmetric algorithm, a new one of said key values in said first and second sequences being produced each time a predetermined number of said blocks are transmitted over said link. Sharebuilder decrypts data sent from the client in order to use the data, and directs the client computer to decrypt data transmitted from the host server in order to provide a useable display to, for example, a user of the client computer. Defendant Sharebuilder is thus liable for infringement of the '730 Patent pursuant to 35 U.S.C. § 271.

111. Upon information and belief, Defendant Morgan Stanley has been and now is directly and jointly infringing, and indirectly infringing by way of inducing infringement and/or contributing to the infringement of the '730 Patent in the State of Texas, in this judicial district, and elsewhere in the United States, by, among other things, methods practiced on various Morgan Stanley websites (including, without limitation, morganstanleyclientserv.com, and ms.com) for transmitting data comprising a sequence of blocks in encrypted form over a communication link covered by one or more claims of the '730 Patent to the injury of TQP. For example, when Morgan Stanley's customers connect to Morgan Stanley's website, a communication link is established between host servers and the client computer. Data transmitted over this communication link comprises a sequence of blocks, and is transmitted as

packets in a sequence over the communication link. Certain data transmissions (both from the client computer to the host server, and from the host server to the client computer) are encrypted according to the claimed method. In order to communicate with encrypted portions of Morgan Stanley's website, client computers must agree to an encryption algorithm or protocol. Once that protocol is established by the host server, the client computer automatically implements the claimed encryption algorithm under the direction of the host server. Morgan Stanley provides, or directs the client computer to provide, a seed value for both the transmitter and receiver in a symmetric encryption algorithm, and uses the same key to encrypt and decrypt data. Morgan Stanley generates, or directs the client computer to generate, a first sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at the transmitter (whichever of the host server or client computer is sending the encrypted information), each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link. Morgan Stanley encrypts data for transmission from the host server to the client. In addition, the Morgan Stanley directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. Morgan Stanley generates, or directs the client computer to generate, a second sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at said receiver, each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link such that said first and second sequences are identical to one another, as is used in a symmetric algorithm, a new one of said key values in said first and second sequences being produced each time a predetermined number of said blocks are transmitted over said link. Morgan Stanley decrypts data sent from the client in order to use the

data, and directs the client computer to decrypt data transmitted from the host server in order to provide a useable display to, for example, a user of the client computer. Defendant Morgan Stanley is thus liable for infringement of the '730 Patent pursuant to 35 U.S.C. § 271.

112. Upon information and belief, Defendant Morgan Stanley Inc. has been and now is directly and jointly infringing, and indirectly infringing by way of inducing infringement and/or contributing to the infringement of the '730 Patent in the State of Texas, in this judicial district, and elsewhere in the United States, by, among other things, methods practiced on various Morgan Stanley Inc. websites (including, without limitation, morganstanleyclientserv.com, and ms.com) for transmitting data comprising a sequence of blocks in encrypted form over a communication link covered by one or more claims of the '730 Patent to the injury of TQP. For example, when Morgan Stanley Inc.'s customers connect to Morgan Stanley Inc.'s website, a communication link is established between host servers and the client computer. Data transmitted over this communication link comprises a sequence of blocks, and is transmitted as packets in a sequence over the communication link. Certain data transmissions (both from the client computer to the host server, and from the host server to the client computer) are encrypted according to the claimed method. In order to communicate with encrypted portions of Morgan Stanley Inc.'s website, client computers must agree to an encryption algorithm or protocol. Once that protocol is established by the host server, the client computer automatically implements the claimed encryption algorithm under the direction of the host server. Morgan Stanley Inc. provides, or directs the client computer to provide, a seed value for both the transmitter and receiver in a symmetric encryption algorithm, and uses the same key to encrypt and decrypt data. Morgan Stanley Inc. generates, or directs the client computer to generate, a first sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on

said seed value at the transmitter (whichever of the host server or client computer is sending the encrypted information), each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link. Morgan Stanley Inc. encrypts data for transmission from the host server to the client. In addition, the Morgan Stanley Inc. directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. Morgan Stanley Inc. generates, or directs the client computer to generate, a second sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at said receiver, each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link such that said first and second sequences are identical to one another, as is used in a symmetric algorithm, a new one of said key values in said first and second sequences being produced each time a predetermined number of said blocks are transmitted over said link. Morgan Stanley Inc. decrypts data sent from the client in order to use the data, and directs the client computer to decrypt data transmitted from the host server in order to provide a useable display to, for example, a user of the client computer. Defendant Morgan Stanley Inc. is thus liable for infringement of the '730 Patent pursuant to 35 U.S.C. § 271.

113. Upon information and belief, Defendant RBS has been and now is directly and jointly infringing, and indirectly infringing by way of inducing infringement and/or contributing to the infringement of the '730 Patent in the State of Texas, in this judicial district, and elsewhere in the United States, by, among other things, methods practiced on various RBS websites (including, without limitation, [citizensbankonline.com](http://citizensbankonline.com), [citizensbankmoneymanagergps.com](http://citizensbankmoneymanagergps.com), [accessmycardonline.com](http://accessmycardonline.com), [charteroneonline.com](http://charteroneonline.com), and [moneymanagergps.com](http://moneymanagergps.com)) for transmitting

data comprising a sequence of blocks in encrypted form over a communication link covered by one or more claims of the '730 Patent to the injury of TQP. For example, when RBS's customers connect to RBS's website, a communication link is established between host servers and the client computer. Data transmitted over this communication link comprises a sequence of blocks, and is transmitted as packets in a sequence over the communication link. Certain data transmissions (both from the client computer to the host server, and from the host server to the client computer) are encrypted according to the claimed method. In order to communicate with encrypted portions of RBS's website, client computers must agree to an encryption algorithm or protocol. Once that protocol is established by the host server, the client computer automatically implements the claimed encryption algorithm under the direction of the host server. RBS provides, or directs the client computer to provide, a seed value for both the transmitter and receiver in a symmetric encryption algorithm, and uses the same key to encrypt and decrypt data. RBS generates, or directs the client computer to generate, a first sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at the transmitter (whichever of the host server or client computer is sending the encrypted information), each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link. RBS encrypts data for transmission from the host server to the client. In addition, the RBS directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. RBS generates, or directs the client computer to generate, a second sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at said receiver, each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted

over said link such that said first and second sequences are identical to one another, as is used in a symmetric algorithm, a new one of said key values in said first and second sequences being produced each time a predetermined number of said blocks are transmitted over said link. RBS decrypts data sent from the client in order to use the data, and directs the client computer to decrypt data transmitted from the host server in order to provide a useable display to, for example, a user of the client computer. Defendant RBS is thus liable for infringement of the '730 Patent pursuant to 35 U.S.C. § 271.

114. Upon information and belief, Defendant Citizens Financial has been and now is directly and jointly infringing, and indirectly infringing by way of inducing infringement and/or contributing to the infringement of the '730 Patent in the State of Texas, in this judicial district, and elsewhere in the United States, by, among other things, methods practiced on various Citizens Financial websites (including, without limitation, [citizensbankonline.com](http://citizensbankonline.com), [citizensbankmoneymanagergps.com](http://citizensbankmoneymanagergps.com), [accessmycardonline.com](http://accessmycardonline.com), [charteroneonline.com](http://charteroneonline.com), and [moneymanagergps.com](http://moneymanagergps.com)) for transmitting data comprising a sequence of blocks in encrypted form over a communication link covered by one or more claims of the '730 Patent to the injury of TQP. For example, when Citizens Financial's customers connect to Citizens Financial's website, a communication link is established between host servers and the client computer. Data transmitted over this communication link comprises a sequence of blocks, and is transmitted as packets in a sequence over the communication link. Certain data transmissions (both from the client computer to the host server, and from the host server to the client computer) are encrypted according to the claimed method. In order to communicate with encrypted portions of Citizens Financial's website, client computers must agree to an encryption algorithm or protocol. Once that protocol is established by the host server, the client computer automatically implements the

claimed encryption algorithm under the direction of the host server. Citizens Financial provides, or directs the client computer to provide, a seed value for both the transmitter and receiver in a symmetric encryption algorithm, and uses the same key to encrypt and decrypt data. Citizens Financial generates, or directs the client computer to generate, a first sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at the transmitter (whichever of the host server or client computer is sending the encrypted information), each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link. Citizens Financial encrypts data for transmission from the host server to the client. In addition, the Citizens Financial directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. Citizens Financial generates, or directs the client computer to generate, a second sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at said receiver, each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link such that said first and second sequences are identical to one another, as is used in a symmetric algorithm, a new one of said key values in said first and second sequences being produced each time a predetermined number of said blocks are transmitted over said link. Citizens Financial decrypts data sent from the client in order to use the data, and directs the client computer to decrypt data transmitted from the host server in order to provide a useable display to, for example, a user of the client computer. Defendant Citizens Financial is thus liable for infringement of the '730 Patent pursuant to 35 U.S.C. § 271.

115. Upon information and belief, Defendant RBS Citizens has been and now is directly and jointly infringing, and indirectly infringing by way of inducing infringement and/or contributing to the infringement of the '730 Patent in the State of Texas, in this judicial district, and elsewhere in the United States, by, among other things, methods practiced on various RBS Citizens websites (including, without limitation, [citizensbankonline.com](http://citizensbankonline.com), [citizensbankmoneymanagergps.com](http://citizensbankmoneymanagergps.com), [accessmycardonline.com](http://accessmycardonline.com), [charteroneonline.com](http://charteroneonline.com), and [moneymanagergps.com](http://moneymanagergps.com)) for transmitting data comprising a sequence of blocks in encrypted form over a communication link covered by one or more claims of the '730 Patent to the injury of TQP. For example, when RBS Citizens' customers connect to RBS Citizens' website, a communication link is established between host servers and the client computer. Data transmitted over this communication link comprises a sequence of blocks, and is transmitted as packets in a sequence over the communication link. Certain data transmissions (both from the client computer to the host server, and from the host server to the client computer) are encrypted according to the claimed method. In order to communicate with encrypted portions of RBS Citizens' website, client computers must agree to an encryption algorithm or protocol. Once that protocol is established by the host server, the client computer automatically implements the claimed encryption algorithm under the direction of the host server. RBS Citizens provides, or directs the client computer to provide, a seed value for both the transmitter and receiver in a symmetric encryption algorithm, and uses the same key to encrypt and decrypt data. RBS Citizens generates, or directs the client computer to generate, a first sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at the transmitter (whichever of the host server or client computer is sending the encrypted information), each new key value in said sequence being produced at a time dependent upon a

predetermined characteristic of the data being transmitted over said link. RBS Citizens encrypts data for transmission from the host server to the client. In addition, the RBS Citizens directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. RBS Citizens generates, or directs the client computer to generate, a second sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at said receiver, each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link such that said first and second sequences are identical to one another, as is used in a symmetric algorithm, a new one of said key values in said first and second sequences being produced each time a predetermined number of said blocks are transmitted over said link. RBS Citizens decrypts data sent from the client in order to use the data, and directs the client computer to decrypt data transmitted from the host server in order to provide a useable display to, for example, a user of the client computer. Defendant RBS Citizens is thus liable for infringement of the '730 Patent pursuant to 35 U.S.C. § 271.

116. Upon information and belief, Defendant Chase has been and now is directly and jointly infringing, and indirectly infringing by way of inducing infringement and/or contributing to the infringement of the '730 Patent in the State of Texas, in this judicial district, and elsewhere in the United States, by, among other things, methods practiced on various Chase websites (including, without limitation, chase.com, and jpmorgan.com) for transmitting data comprising a sequence of blocks in encrypted form over a communication link covered by one or more claims of the '730 Patent to the injury of TQP. For example, when Chase's customers connect to Chase's website, a communication link is established between host servers and the client computer. Data transmitted over this communication link comprises a sequence of blocks, and is

transmitted as packets in a sequence over the communication link. Certain data transmissions (both from the client computer to the host server, and from the host server to the client computer) are encrypted according to the claimed method. In order to communicate with encrypted portions of Chase's website, client computers must agree to an encryption algorithm or protocol. Once that protocol is established by the host server, the client computer automatically implements the claimed encryption algorithm under the direction of the host server. Chase provides, or directs the client computer to provide, a seed value for both the transmitter and receiver in a symmetric encryption algorithm, and uses the same key to encrypt and decrypt data. Chase generates, or directs the client computer to generate, a first sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at the transmitter (whichever of the host server or client computer is sending the encrypted information), each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link. Chase encrypts data for transmission from the host server to the client. In addition, the Chase directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. Chase generates, or directs the client computer to generate, a second sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at said receiver, each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link such that said first and second sequences are identical to one another, as is used in a symmetric algorithm, a new one of said key values in said first and second sequences being produced each time a predetermined number of said blocks are transmitted over said link. Chase decrypts data sent from the client in order to use the data, and directs the client computer to

decrypt data transmitted from the host server in order to provide a useable display to, for example, a user of the client computer. Defendant Chase is thus liable for infringement of the '730 Patent pursuant to 35 U.S.C. § 271.

117. Upon information and belief, Defendant Chase Bank has been and now is directly and jointly infringing, and indirectly infringing by way of inducing infringement and/or contributing to the infringement of the '730 Patent in the State of Texas, in this judicial district, and elsewhere in the United States, by, among other things, methods practiced on various Chase Bank websites (including, without limitation, chase.com, and jpmorgan.com) for transmitting data comprising a sequence of blocks in encrypted form over a communication link covered by one or more claims of the '730 Patent to the injury of TQP. For example, when Chase Bank's customers connect to Chase Bank's website, a communication link is established between host servers and the client computer. Data transmitted over this communication link comprises a sequence of blocks, and is transmitted as packets in a sequence over the communication link. Certain data transmissions (both from the client computer to the host server, and from the host server to the client computer) are encrypted according to the claimed method. In order to communicate with encrypted portions of Chase Bank's website, client computers must agree to an encryption algorithm or protocol. Once that protocol is established by the host server, the client computer automatically implements the claimed encryption algorithm under the direction of the host server. Chase Bank provides, or directs the client computer to provide, a seed value for both the transmitter and receiver in a symmetric encryption algorithm, and uses the same key to encrypt and decrypt data. Chase Bank generates, or directs the client computer to generate, a first sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at the transmitter (whichever of the host server or client

computer is sending the encrypted information), each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link. Chase Bank encrypts data for transmission from the host server to the client. In addition, the Chase Bank directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. Chase Bank generates, or directs the client computer to generate, a second sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at said receiver, each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link such that said first and second sequences are identical to one another, as is used in a symmetric algorithm, a new one of said key values in said first and second sequences being produced each time a predetermined number of said blocks are transmitted over said link. Chase Bank decrypts data sent from the client in order to use the data, and directs the client computer to decrypt data transmitted from the host server in order to provide a useable display to, for example, a user of the client computer. Defendant Chase Bank is thus liable for infringement of the '730 Patent pursuant to 35 U.S.C. § 271.

118. Upon information and belief, Defendant Raymond James has been and now is directly and jointly infringing, and indirectly infringing by way of inducing infringement and/or contributing to the infringement of the '730 Patent in the State of Texas, in this judicial district, and elsewhere in the United States, by, among other things, methods practiced on various Raymond James websites (including, without limitation, rtf.com, and rjbank.com) for transmitting data comprising a sequence of blocks in encrypted form over a communication link covered by one or more claims of the '730 Patent to the injury of TQP. For example, when

Raymond James' customers connect to Raymond James' website, a communication link is established between host servers and the client computer. Data transmitted over this communication link comprises a sequence of blocks, and is transmitted as packets in a sequence over the communication link. Certain data transmissions (both from the client computer to the host server, and from the host server to the client computer) are encrypted according to the claimed method. In order to communicate with encrypted portions of Raymond James' website, client computers must agree to an encryption algorithm or protocol. Once that protocol is established by the host server, the client computer automatically implements the claimed encryption algorithm under the direction of the host server. Raymond James provides, or directs the client computer to provide, a seed value for both the transmitter and receiver in a symmetric encryption algorithm, and uses the same key to encrypt and decrypt data. Raymond James generates, or directs the client computer to generate, a first sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at the transmitter (whichever of the host server or client computer is sending the encrypted information), each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link. Raymond James encrypts data for transmission from the host server to the client. In addition, the Raymond James directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. Raymond James generates, or directs the client computer to generate, a second sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at said receiver, each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link such that said first and second sequences are identical

to one another, as is used in a symmetric algorithm, a new one of said key values in said first and second sequences being produced each time a predetermined number of said blocks are transmitted over said link. Raymond James decrypts data sent from the client in order to use the data, and directs the client computer to decrypt data transmitted from the host server in order to provide a useable display to, for example, a user of the client computer. Defendant Raymond James is thus liable for infringement of the '730 Patent pursuant to 35 U.S.C. § 271.

119. Upon information and belief, Defendant TD AMERITRADE Holding has been and now is directly and jointly infringing, and indirectly infringing by way of inducing infringement and/or contributing to the infringement of the '730 Patent in the State of Texas, in this judicial district, and elsewhere in the United States, by, among other things, methods practiced on various TD AMERITRADE Holding websites (including, without limitation, ameritrade.com, and tdameritrade.com) for transmitting data comprising a sequence of blocks in encrypted form over a communication link covered by one or more claims of the '730 Patent to the injury of TQP. For example, when TD AMERITRADE Holding's customers connect to TD AMERITRADE Holding's website, a communication link is established between host servers and the client computer. Data transmitted over this communication link comprises a sequence of blocks, and is transmitted as packets in a sequence over the communication link. Certain data transmissions (both from the client computer to the host server, and from the host server to the client computer) are encrypted according to the claimed method. In order to communicate with encrypted portions of TD AMERITRADE Holding's website, client computers must agree to an encryption algorithm or protocol. Once that protocol is established by the host server, the client computer automatically implements the claimed encryption algorithm under the direction of the host server. TD AMERITRADE Holding provides, or directs the client computer to provide, a

seed value for both the transmitter and receiver in a symmetric encryption algorithm, and uses the same key to encrypt and decrypt data. TD AMERITRADE Holding generates, or directs the client computer to generate, a first sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at the transmitter (whichever of the host server or client computer is sending the encrypted information), each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link. TD AMERITRADE Holding encrypts data for transmission from the host server to the client. In addition, the TD AMERITRADE Holding directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. TD AMERITRADE Holding generates, or directs the client computer to generate, a second sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at said receiver, each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link such that said first and second sequences are identical to one another, as is used in a symmetric algorithm, a new one of said key values in said first and second sequences being produced each time a predetermined number of said blocks are transmitted over said link. TD AMERITRADE Holding decrypts data sent from the client in order to use the data, and directs the client computer to decrypt data transmitted from the host server in order to provide a useable display to, for example, a user of the client computer. Defendant TD AMERITRADE Holding is thus liable for infringement of the '730 Patent pursuant to 35 U.S.C. § 271.

120. Upon information and belief, Defendant TD AMERITRADE has been and now is directly and jointly infringing, and indirectly infringing by way of inducing infringement and/or

contributing to the infringement of the '730 Patent in the State of Texas, in this judicial district, and elsewhere in the United States, by, among other things, methods practiced on various TD AMERITRADE websites (including, without limitation, ameritrade.com, and tdameritrade.com) for transmitting data comprising a sequence of blocks in encrypted form over a communication link covered by one or more claims of the '730 Patent to the injury of TQP. For example, when TD AMERITRADE's customers connect to TD AMERITRADE's website, a communication link is established between host servers and the client computer. Data transmitted over this communication link comprises a sequence of blocks, and is transmitted as packets in a sequence over the communication link. Certain data transmissions (both from the client computer to the host server, and from the host server to the client computer) are encrypted according to the claimed method. In order to communicate with encrypted portions of TD AMERITRADE's website, client computers must agree to an encryption algorithm or protocol. Once that protocol is established by the host server, the client computer automatically implements the claimed encryption algorithm under the direction of the host server. TD AMERITRADE provides, or directs the client computer to provide, a seed value for both the transmitter and receiver in a symmetric encryption algorithm, and uses the same key to encrypt and decrypt data. TD AMERITRADE generates, or directs the client computer to generate, a first sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at the transmitter (whichever of the host server or client computer is sending the encrypted information), each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link. TD AMERITRADE encrypts data for transmission from the host server to the client. In addition, the TD AMERITRADE directs the client computer to encrypt data comprising information sent from

the client to the host server before it is transmitted over the link. TD AMERITRADE generates, or directs the client computer to generate, a second sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at said receiver, each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link such that said first and second sequences are identical to one another, as is used in a symmetric algorithm, a new one of said key values in said first and second sequences being produced each time a predetermined number of said blocks are transmitted over said link. TD AMERITRADE decrypts data sent from the client in order to use the data, and directs the client computer to decrypt data transmitted from the host server in order to provide a useable display to, for example, a user of the client computer. Defendant TD AMERITRADE is thus liable for infringement of the '730 Patent pursuant to 35 U.S.C. § 271.

121. Upon information and belief, Defendant Regions has been and now is directly and jointly infringing, and indirectly infringing by way of inducing infringement and/or contributing to the infringement of the '730 Patent in the State of Texas, in this judicial district, and elsewhere in the United States, by, among other things, methods practiced on various Regions websites (including, without limitation, regions.com) for transmitting data comprising a sequence of blocks in encrypted form over a communication link covered by one or more claims of the '730 Patent to the injury of TQP. For example, when Regions and/or Regions' customers connect to Regions' website, a communication link is established between host servers and the client computer. Data transmitted over this communication link comprises a sequence of blocks, and is transmitted as packets in a sequence over the communication link. Certain data transmissions (both from the client computer to the host server, and from the host server to the client computer)

are encrypted according to the claimed method. In order to communicate with encrypted portions of Regions' website, client computers must agree to an encryption algorithm or protocol. Once that protocol is established by the host server, the client computer automatically implements the claimed encryption algorithm under the direction of the host server. Regions provides, or directs the client computer to provide, a seed value for both the transmitter and receiver in a symmetric encryption algorithm, and uses the same key to encrypt and decrypt data. Regions generates, or directs the client computer to generate, a first sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at the transmitter (whichever of the host server or client computer is sending the encrypted information), each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link. Regions encrypts data for transmission from the host server to the client. In addition, the Regions directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. Regions generates, or directs the client computer to generate, a second sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at said receiver, each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link such that said first and second sequences are identical to one another, as is used in a symmetric algorithm, a new one of said key values in said first and second sequences being produced each time a predetermined number of said blocks are transmitted over said link. Regions decrypts data sent from the client in order to use the data, and directs the client computer to decrypt data transmitted from the host server in order to provide a useable display

to, for example, a user of the client computer. Defendant Regions is thus liable for infringement of the '730 Patent pursuant to 35 U.S.C. § 271.

122. Upon information and belief, Defendant National City has been and now is directly and jointly infringing, and indirectly infringing by way of inducing infringement and/or contributing to the infringement of the '730 Patent in the State of Texas, in this judicial district, and elsewhere in the United States, by, among other things, methods practiced on various National City websites (including, without limitation, [nationalcityhomeloans.com](http://nationalcityhomeloans.com)) for transmitting data comprising a sequence of blocks in encrypted form over a communication link covered by one or more claims of the '730 Patent to the injury of TQP. For example, when National City and/or National City's customers connect to National City's website, a communication link is established between host servers and the client computer. Data transmitted over this communication link comprises a sequence of blocks, and is transmitted as packets in a sequence over the communication link. Certain data transmissions (both from the client computer to the host server, and from the host server to the client computer) are encrypted according to the claimed method. In order to communicate with encrypted portions of National City's website, client computers must agree to an encryption algorithm or protocol. Once that protocol is established by the host server, the client computer automatically implements the claimed encryption algorithm under the direction of the host server. National City provides, or directs the client computer to provide, a seed value for both the transmitter and receiver in a symmetric encryption algorithm, and uses the same key to encrypt and decrypt data. National City generates, or directs the client computer to generate, a first sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at the transmitter (whichever of the host server or client computer is sending the encrypted

information), each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link. National City encrypts data for transmission from the host server to the client. In addition, the National City directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. National City generates, or directs the client computer to generate, a second sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at said receiver, each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link such that said first and second sequences are identical to one another, as is used in a symmetric algorithm, a new one of said key values in said first and second sequences being produced each time a predetermined number of said blocks are transmitted over said link. National City decrypts data sent from the client in order to use the data, and directs the client computer to decrypt data transmitted from the host server in order to provide a useable display to, for example, a user of the client computer. Defendant National City is thus liable for infringement of the '730 Patent pursuant to 35 U.S.C. § 271.

123. Upon information and belief, Defendant National City Bank has been and now is directly and jointly infringing, and indirectly infringing by way of inducing infringement and/or contributing to the infringement of the '730 Patent in the State of Texas, in this judicial district, and elsewhere in the United States, by, among other things, methods practiced on various National Bank websites (including, without limitation, nationalcityhomeloans.com) for transmitting data comprising a sequence of blocks in encrypted form over a communication link covered by one or more claims of the '730 Patent to the injury of TQP. For example, when National Bank and/or National Bank's customers connect to National Bank's website, a

communication link is established between host servers and the client computer. Data transmitted over this communication link comprises a sequence of blocks, and is transmitted as packets in a sequence over the communication link. Certain data transmissions (both from the client computer to the host server, and from the host server to the client computer) are encrypted according to the claimed method. In order to communicate with encrypted portions of National Bank's website, client computers must agree to an encryption algorithm or protocol. Once that protocol is established by the host server, the client computer automatically implements the claimed encryption algorithm under the direction of the host server. National Bank provides, or directs the client computer to provide, a seed value for both the transmitter and receiver in a symmetric encryption algorithm, and uses the same key to encrypt and decrypt data. National Bank generates, or directs the client computer to generate, a first sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at the transmitter (whichever of the host server or client computer is sending the encrypted information), each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link. National Bank encrypts data for transmission from the host server to the client. In addition, the National Bank directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. National Bank generates, or directs the client computer to generate, a second sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at said receiver, each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link such that said first and second sequences are identical to one another, as is used in a symmetric algorithm, a new one of said key values in said first and

second sequences being produced each time a predetermined number of said blocks are transmitted over said link. National Bank decrypts data sent from the client in order to use the data, and directs the client computer to decrypt data transmitted from the host server in order to provide a useable display to, for example, a user of the client computer. Defendant National Bank is thus liable for infringement of the '730 Patent pursuant to 35 U.S.C. § 271.

124. Upon information and belief, Defendant IBC has been and now is directly and jointly infringing, and indirectly infringing by way of inducing infringement and/or contributing to the infringement of the '730 Patent in the State of Texas, in this judicial district, and elsewhere in the United States, by, among other things, methods practiced on various IBC websites (including, without limitation, ibc.com) for transmitting data comprising a sequence of blocks in encrypted form over a communication link covered by one or more claims of the '730 Patent to the injury of TQP. For example, when IBC and/or IBC's customers connect to IBC's website, a communication link is established between host servers and the client computer. Data transmitted over this communication link comprises a sequence of blocks, and is transmitted as packets in a sequence over the communication link. Certain data transmissions (both from the client computer to the host server, and from the host server to the client computer) are encrypted according to the claimed method. In order to communicate with encrypted portions of IBC's website, client computers must agree to an encryption algorithm or protocol. Once that protocol is established by the host server, the client computer automatically implements the claimed encryption algorithm under the direction of the host server. IBC provides, or directs the client computer to provide, a seed value for both the transmitter and receiver in a symmetric encryption algorithm, and uses the same key to encrypt and decrypt data. IBC generates, or directs the client computer to generate, a first sequence of pseudo-random key values, such as alpha and/or

numerical values used to encrypt data, based on said seed value at the transmitter (whichever of the host server or client computer is sending the encrypted information), each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link. IBC encrypts data for transmission from the host server to the client. In addition, the IBC directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. IBC generates, or directs the client computer to generate, a second sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at said receiver, each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link such that said first and second sequences are identical to one another, as is used in a symmetric algorithm, a new one of said key values in said first and second sequences being produced each time a predetermined number of said blocks are transmitted over said link. IBC decrypts data sent from the client in order to use the data, and directs the client computer to decrypt data transmitted from the host server in order to provide a useable display to, for example, a user of the client computer. Defendant IBC is thus liable for infringement of the '730 Patent pursuant to 35 U.S.C. § 271.

125. Upon information and belief, Defendant IBC Subsidiary has been and now is directly and jointly infringing, and indirectly infringing by way of inducing infringement and/or contributing to the infringement of the '730 Patent in the State of Texas, in this judicial district, and elsewhere in the United States, by, among other things, methods practiced on various IBC Subsidiary websites (including, without limitation, ibc.com) for transmitting data comprising a sequence of blocks in encrypted form over a communication link covered by one or more claims of the '730 Patent to the injury of TQP. For example, when IBC Subsidiary and/or IBC

Subsidiary's customers connect to IBC Subsidiary's website, a communication link is established between host servers and the client computer. Data transmitted over this communication link comprises a sequence of blocks, and is transmitted as packets in a sequence over the communication link. Certain data transmissions (both from the client computer to the host server, and from the host server to the client computer) are encrypted according to the claimed method. In order to communicate with encrypted portions of IBC Subsidiary's website, client computers must agree to an encryption algorithm or protocol. Once that protocol is established by the host server, the client computer automatically implements the claimed encryption algorithm under the direction of the host server. IBC Subsidiary provides, or directs the client computer to provide, a seed value for both the transmitter and receiver in a symmetric encryption algorithm, and uses the same key to encrypt and decrypt data. IBC Subsidiary generates, or directs the client computer to generate, a first sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at the transmitter (whichever of the host server or client computer is sending the encrypted information), each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link. IBC Subsidiary encrypts data for transmission from the host server to the client. In addition, the IBC Subsidiary directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. IBC Subsidiary generates, or directs the client computer to generate, a second sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at said receiver, each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link such that said first and second sequences are identical to one another,

as is used in a symmetric algorithm, a new one of said key values in said first and second sequences being produced each time a predetermined number of said blocks are transmitted over said link. IBC Subsidiary decrypts data sent from the client in order to use the data, and directs the client computer to decrypt data transmitted from the host server in order to provide a useable display to, for example, a user of the client computer. Defendant IBC Subsidiary is thus liable for infringement of the '730 Patent pursuant to 35 U.S.C. § 271.

126. Upon information and belief, Defendant IBC Bank has been and now is directly and jointly infringing, and indirectly infringing by way of inducing infringement and/or contributing to the infringement of the '730 Patent in the State of Texas, in this judicial district, and elsewhere in the United States, by, among other things, methods practiced on various IBC Bank websites (including, without limitation, [ibc.com](http://ibc.com)) for transmitting data comprising a sequence of blocks in encrypted form over a communication link covered by one or more claims of the '730 Patent to the injury of TQP. For example, when IBC Bank and/or IBC Bank's customers connect to IBC Bank's website, a communication link is established between host servers and the client computer. Data transmitted over this communication link comprises a sequence of blocks, and is transmitted as packets in a sequence over the communication link. Certain data transmissions (both from the client computer to the host server, and from the host server to the client computer) are encrypted according to the claimed method. In order to communicate with encrypted portions of IBC Bank's website, client computers must agree to an encryption algorithm or protocol. Once that protocol is established by the host server, the client computer automatically implements the claimed encryption algorithm under the direction of the host server. IBC Bank provides, or directs the client computer to provide, a seed value for both the transmitter and receiver in a symmetric encryption algorithm, and uses the same key to

encrypt and decrypt data. IBC Bank generates, or directs the client computer to generate, a first sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at the transmitter (whichever of the host server or client computer is sending the encrypted information), each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link. IBC Bank encrypts data for transmission from the host server to the client. In addition, the IBC Bank directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. IBC Bank generates, or directs the client computer to generate, a second sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at said receiver, each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link such that said first and second sequences are identical to one another, as is used in a symmetric algorithm, a new one of said key values in said first and second sequences being produced each time a predetermined number of said blocks are transmitted over said link. IBC Bank decrypts data sent from the client in order to use the data, and directs the client computer to decrypt data transmitted from the host server in order to provide a useable display to, for example, a user of the client computer. Defendant IBC Bank is thus liable for infringement of the '730 Patent pursuant to 35 U.S.C. § 271.

127. Upon information and belief, Defendant Amegy has been and now is directly and jointly infringing, and indirectly infringing by way of inducing infringement and/or contributing to the infringement of the '730 Patent in the State of Texas, in this judicial district, and elsewhere in the United States, by, among other things, methods practiced on various Amegy websites (including, without limitation, amegybank.com) for transmitting data comprising a sequence of

blocks in encrypted form over a communication link covered by one or more claims of the '730 Patent to the injury of TQP. For example, when Amegy and/or Amegy's customers connect to Amegy's website, a communication link is established between host servers and the client computer. Data transmitted over this communication link comprises a sequence of blocks, and is transmitted as packets in a sequence over the communication link. Certain data transmissions (both from the client computer to the host server, and from the host server to the client computer) are encrypted according to the claimed method. In order to communicate with encrypted portions of Amegy's website, client computers must agree to an encryption algorithm or protocol. Once that protocol is established by the host server, the client computer automatically implements the claimed encryption algorithm under the direction of the host server. Amegy provides, or directs the client computer to provide, a seed value for both the transmitter and receiver in a symmetric encryption algorithm, and uses the same key to encrypt and decrypt data. Amegy generates, or directs the client computer to generate, a first sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at the transmitter (whichever of the host server or client computer is sending the encrypted information), each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link. Amegy encrypts data for transmission from the host server to the client. In addition, the Amegy directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. Amegy generates, or directs the client computer to generate, a second sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at said receiver, each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being

transmitted over said link such that said first and second sequences are identical to one another, as is used in a symmetric algorithm, a new one of said key values in said first and second sequences being produced each time a predetermined number of said blocks are transmitted over said link. Amegy decrypts data sent from the client in order to use the data, and directs the client computer to decrypt data transmitted from the host server in order to provide a useable display to, for example, a user of the client computer. Defendant Amegy is thus liable for infringement of the '730 Patent pursuant to 35 U.S.C. § 271.

128. Upon information and belief, Defendant Amegy Bank has been and now is directly and jointly infringing, and indirectly infringing by way of inducing infringement and/or contributing to the infringement of the '730 Patent in the State of Texas, in this judicial district, and elsewhere in the United States, by, among other things, methods practiced on various Amegy Bank websites (including, without limitation, amegybank.com) for transmitting data comprising a sequence of blocks in encrypted form over a communication link covered by one or more claims of the '730 Patent to the injury of TQP. For example, when Amegy Bank and/or Amegy Bank's customers connect to Amegy Bank's website, a communication link is established between host servers and the client computer. Data transmitted over this communication link comprises a sequence of blocks, and is transmitted as packets in a sequence over the communication link. Certain data transmissions (both from the client computer to the host server, and from the host server to the client computer) are encrypted according to the claimed method. In order to communicate with encrypted portions of Amegy Bank's website, client computers must agree to an encryption algorithm or protocol. Once that protocol is established by the host server, the client computer automatically implements the claimed encryption algorithm under the direction of the host server. Amegy Bank provides, or directs the

client computer to provide, a seed value for both the transmitter and receiver in a symmetric encryption algorithm, and uses the same key to encrypt and decrypt data. Amegy Bank generates, or directs the client computer to generate, a first sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at the transmitter (whichever of the host server or client computer is sending the encrypted information), each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link. Amegy Bank encrypts data for transmission from the host server to the client. In addition, the Amegy Bank directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. Amegy Bank generates, or directs the client computer to generate, a second sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at said receiver, each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link such that said first and second sequences are identical to one another, as is used in a symmetric algorithm, a new one of said key values in said first and second sequences being produced each time a predetermined number of said blocks are transmitted over said link. Amegy Bank decrypts data sent from the client in order to use the data, and directs the client computer to decrypt data transmitted from the host server in order to provide a useable display to, for example, a user of the client computer. Defendant Amegy Bank is thus liable for infringement of the '730 Patent pursuant to 35 U.S.C. § 271.

129. Upon information and belief, Defendant Fifth Third has been and now is directly and jointly infringing, and indirectly infringing by way of inducing infringement and/or contributing to the infringement of the '730 Patent in the State of Texas, in this judicial district,

and elsewhere in the United States, by, among other things, methods practiced on various Fifth Third websites (including, without limitation, 53.com) for transmitting data comprising a sequence of blocks in encrypted form over a communication link covered by one or more claims of the '730 Patent to the injury of TQP. For example, when Fifth Third and/or Fifth Third's customers connect to Fifth Third's website, a communication link is established between host servers and the client computer. Data transmitted over this communication link comprises a sequence of blocks, and is transmitted as packets in a sequence over the communication link. Certain data transmissions (both from the client computer to the host server, and from the host server to the client computer) are encrypted according to the claimed method. In order to communicate with encrypted portions of Fifth Third's website, client computers must agree to an encryption algorithm or protocol. Once that protocol is established by the host server, the client computer automatically implements the claimed encryption algorithm under the direction of the host server. Fifth Third provides, or directs the client computer to provide, a seed value for both the transmitter and receiver in a symmetric encryption algorithm, and uses the same key to encrypt and decrypt data. Fifth Third generates, or directs the client computer to generate, a first sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at the transmitter (whichever of the host server or client computer is sending the encrypted information), each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link. Fifth Third encrypts data for transmission from the host server to the client. In addition, the Fifth Third directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. Fifth Third generates, or directs the client computer to generate, a second sequence of pseudo-random key values, such as alpha and/or

numerical values used to encrypt data, based on said seed value at said receiver, each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link such that said first and second sequences are identical to one another, as is used in a symmetric algorithm, a new one of said key values in said first and second sequences being produced each time a predetermined number of said blocks are transmitted over said link. Fifth Third decrypts data sent from the client in order to use the data, and directs the client computer to decrypt data transmitted from the host server in order to provide a useable display to, for example, a user of the client computer. Defendant Fifth Third is thus liable for infringement of the '730 Patent pursuant to 35 U.S.C. § 271.

130. Upon information and belief, Defendant Fifth Third Bank Third Bank has been and now is directly and jointly infringing, and indirectly infringing by way of inducing infringement and/or contributing to the infringement of the '730 Patent in the State of Texas, in this judicial district, and elsewhere in the United States, by, among other things, methods practiced on various Fifth Third Bank websites (including, without limitation, 53.com) for transmitting data comprising a sequence of blocks in encrypted form over a communication link covered by one or more claims of the '730 Patent to the injury of TQP. For example, when Fifth Third Bank and/or Fifth Third Bank's customers connect to Fifth Third Bank's website, a communication link is established between host servers and the client computer. Data transmitted over this communication link comprises a sequence of blocks, and is transmitted as packets in a sequence over the communication link. Certain data transmissions (both from the client computer to the host server, and from the host server to the client computer) are encrypted according to the claimed method. In order to communicate with encrypted portions of Fifth Third Bank's website, client computers must agree to an encryption algorithm or protocol. Once

that protocol is established by the host server, the client computer automatically implements the claimed encryption algorithm under the direction of the host server. Fifth Third Bank provides, or directs the client computer to provide, a seed value for both the transmitter and receiver in a symmetric encryption algorithm, and uses the same key to encrypt and decrypt data. Fifth Third Bank generates, or directs the client computer to generate, a first sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at the transmitter (whichever of the host server or client computer is sending the encrypted information), each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link. Fifth Third Bank encrypts data for transmission from the host server to the client. In addition, the Fifth Third Bank directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. Fifth Third Bank generates, or directs the client computer to generate, a second sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at said receiver, each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link such that said first and second sequences are identical to one another, as is used in a symmetric algorithm, a new one of said key values in said first and second sequences being produced each time a predetermined number of said blocks are transmitted over said link. Fifth Third Bank decrypts data sent from the client in order to use the data, and directs the client computer to decrypt data transmitted from the host server in order to provide a useable display to, for example, a user of the client computer. Defendant Fifth Third Bank is thus liable for infringement of the '730 Patent pursuant to 35 U.S.C. § 271.

131. On information and belief, all predecessors in interest to the '730 Patent complied with any marking requirements required by 35 U.S.C. § 287.

132. To the extent that facts learned in discovery show that Defendants' infringement of the '730 patent is or has been willful, Plaintiff reserves the right to request such a finding.

133. As a result of these Defendants' infringement of the '730 Patent, Plaintiff has suffered monetary damages in an amount adequate to compensate for Defendants' infringement, but in no event less than a reasonable royalty for the use made of the invention by Defendants, together with interest and costs as fixed by the court, and Plaintiff will continue to suffer damages in the future unless Defendants' infringing activities are enjoined by this Court.

134. Unless a permanent injunction is issued enjoining these Defendants and their agents, servants, employees, representatives, affiliates, and all others acting in active concert therewith from infringing the '730 Patent, Plaintiff will be greatly and irreparably harmed.

#### **PRAYER FOR RELIEF**

WHEREFORE, Plaintiff respectfully requests that this Court enter:

1. A judgment in favor of Plaintiff that Defendants have infringed, directly and jointly, jointly, and/or indirectly, by way of inducing and/or contributing to the infringement of the '730 Patent, and that such infringement was willful;

2. A permanent injunction enjoining Defendants and their officers, directors, agents, servants, affiliates, employees, divisions, branches, subsidiaries, parents, and all others acting in active concert therewith from infringement, inducing the infringement of, or contributing to the infringement of the '730 Patent;

3. A judgment and order requiring Defendants to pay Plaintiff its damages, costs, expenses, and prejudgment and post-judgment interest for Defendants' infringement of the '730 Patent as provided under 35 U.S.C. § 284;

4. A judgment and order finding that this is an exceptional case within the meaning of 35 U.S.C. § 285 and awarding to Plaintiff its reasonable attorneys' fees; and

5. Any and all other relief to which Plaintiff may show itself to be entitled.

**DEMAND FOR JURY TRIAL**

Plaintiff, under Rule 38 of the Federal Rules of Civil Procedure, requests a trial by jury of any issues so triable by right.

Respectfully submitted,

**TQP DEVELOPMENT, LLC**

Dated: December 15, 2008

By: /s/Marc A. Fenster  
Kip Glasscock - LEAD COUNSEL  
Texas Bar No. 08011000  
Kip Glasscock, P.C.  
550 Fannin Suite 1350  
(409) 833-8822  
Beaumont, TX, 77701

Marc A. Fenster  
California Bar No. 181067  
E-mail: mfenster@raklaw.com  
RUSS, AUGUST & KABAT  
12424 Wilshire Boulevard 12th Floor  
Los Angeles, California 90025  
Telephone: 310/826-7474  
Facsimile: 310/826-6991

**ATTORNEYS FOR PLAINTIFF  
TQP DEVELOPMENT, LLC**